


جامعة القاهرة

كليه الاقتصاد والعلوم السياسية

قسم العلوم السياسية


# أثر الإرهاب الالكتروني على مبدأ استخدام القوة في العلاقات الدولية

رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في العلوم السياسية


إعداد الطالب

عادل عبد الصادق محمد الجخة

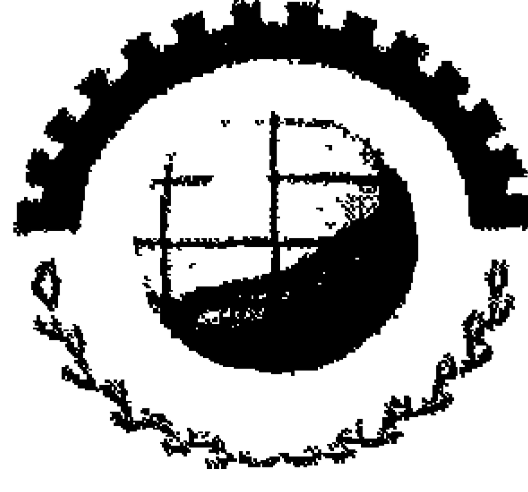
إشراف

أ.د / احمد عبد الونيس شتا

أستاذ العلوم السياسية والقانون الدولي بجامعه القاهرة


٢٠٠٩





جامعة القاهرة
كليه الاقتصاد والعلوم السياسية
قسم العلوم السياسية

---

# أثر الإرهاب الإلكتروني على مبدأ استخدام القوة في العلاقات الدولية

## [٢٠٠١-٢٠٠٧]

---

رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في العلوم السياسية

إعداد الطالب

عـادل عبـد الصـادق محمـد الجَخـة

إشراف

أ.د / احمـد عبـد الونيـس شتـا

أستاذ العلوم السياسية والقانون الدولي بجامعه القاهرة

٢٠٠٩

# الاجازة

اجازت لجنة المناقشة هذه الرسالة للحصول على درجة الماجستير في العلوم السياسية ومنحت الطالب تقدير ممتاز في الرسالة المقدمة وتقدير عام / جيد جدا بتاريخ / ٢٠٠٩/٣/١٢ بعد استيفاء جميع المتطلبات.

| اللجنة | | |
|---|---|---|
| أ.د احمد عبد الونيس شتا | استاذ العلوم السياسية والقانون الدولي<br>[ مشرفا ورئيسا ] | |
| أ. د احمد حسن الرشيدي | وكيل كلية الاقتصاد لشئون الدراسات العليا واستاذ القانون الدولي والعلوم السياسية<br>[ عضوا من الداخل ] | أحمد الرشيدي |
| ل. د محمود محمد خلف | الخبير الاستراتيجي ومستشار اكاديمية ناصر العسكرية العليا<br>[ عضوا من الخارج ] | |



# إهداء

إلى روح أبي وعطاء أمي الفياض

أكبر قلبين باركا طموحي بالرعاية والصبر

فجزاهما الله عني خير الجزاء .



# الشكر

الحمد لله الذي وفقني وأعانني على إتمام هذه الدراسة، والذي كان من توفيقه أن أتاح لي من وقف بجانبي من رجال صدقوا ما عاهدوا الله عليه وأخص بالشكر الجزيل العالم والإنسان الأستاذ الدكتور احمد عبد الونيس شتا على ما قدمه لي من عون ومساندة في مراحل إعداد هذه الدراسة، حيث تبنى الفكرة وشجع على إنجازها رغم جدة الموضوع، كما أتوجه بالشكر الى الاستاذ الدكتور احمد حسن الرشيدي وكيل كلية الاقتصاد والعلوم السياسية لشؤون الدراسات العليا، وأستاذ القانون الدولي والعلوم السياسية بالكلية، كما اشكر السيد اللواء دكتور محمود محمد خلف الخبير الاستراتيجي ومستشار أكاديمية ناصر العسكرية العليا . على موافقتهما على فحص جهدي المتواضع ومساهمة ارائهم وملاحظتهم في اثراء هذا العمل .

وا أتوجه بالشكر إلى كوكبة من الأساتذة والسادة الزملاء والأصدقاء على ما قدموه لي من دعم ومساندة خلال إعداد هذا العمل، وعلى رأسهم الأستاذ السيد يسن مستشار مركز الدراسات السياسية والاستراتيجية بالأهرام، كما اشكر د . عبد المنعم سعيد مدير مركز الدراسات السياسية والإستراتيجية بالأهرام على ما قدم لي من دعم، كما اشكر د . حسن أبو طالب مساعد مدير المركز ورئيس وحدة دراسات الانترنت بمركز الدراسات السياسية والإستراتيجية بالأهرام ،واقدم شكري لجميع من قدموا لي العون على أي وجه من الأوجه، ولم أرهم أو اذكرهم شكرا موفورا غير منقوص . . راجيا أن يجزيهم الله خير الجزاء ويمتعهم بموفور الصحة والعافية . إنه نعم المولى إنه سميع مجيب .

| الصفحة | قائمة المحتويات: |
|---|---|
|  |

## مقدمة:

### أولا: تحديد موضوع الدراسة.

يدور موضوع هذه الدراسة حول بيان واستجلاء الآثار والتداعيات المترتبة على ظاهرة الإرهاب الالكتروني التي تنامت في ظل الثورة العلمية والمعلوماتية الحاصلة في الآونة الراهنة بالنسبة إلى استخدام القوة في العلاقات الدولية، سواء فيما يختص بعلاقة هذا بطبيعة القوة أو فيما يتعلق بمضمونها وأبعادها، ومدى تأثير ذلك كله على أنماط وحالات الصراع والسلم في العلاقات الدولية المعاصرة.

وجاء ذلك بعد ان طرحت مسألة الثورة العلمية والتكنولوجية تجلياتها على المجالات كافة بشكل جعلها أكثر ملاءمة ومعايشة بتحولها من الطور النظري إلى الطور العملي الذي شكل ويحق فرصة مهمة في تطور الفكر الإنساني والحياة المعاصرة وفتحت آفاقا رحبة أمام مستقبل التطور الإنساني.

وكان من أحد ملامح الثورة التكنولوجية ظاهرة الفضاء الالكتروني والتي أصبح لها دورا استراتيجيا في المجتمع الدولي على الصعيد الاقتصادي والسياسي والثقافي والأمني والاجتماعي، والى جانب ذلك ظهرت استخدامات أخرى غير سلمية تعبر عن التزاوج ما بين تكنولوجيا الاتصال والمعلومات والإرهاب والحرب ليعبر ذلك عن إحدى القضايا الدولية المعقدة في العصر الحديث، ليس فقط في الإشكاليات التي تفرضها ولكن أيضا في التكتيكات والاستراتيجيات وطبيعة التحديات أمام كافة الفاعلين من الدول والجماعات والأفراد داخل مجتمع المعلومات العالمي .

وأصبح ذلك الظهور الجديد للقوة في العلاقات الدولية أكثر قابلية للاستخدام والانتشار والتأثير عن غيرها من أنواع القوة الصلبة ، وتميزت تلك القوة بتعدد أنماطها وأدواتها وسهولة استخدامها، وظهر ذلك في صورة الإرهاب الالكتروني وحرب المعلومات وغيرها من المظاهر التي تتضمن استخداما غير سلمي للفضاء الالكتروني و بما جعل العالم أمام تزايد المصالح الحيوية، وفي ذات الوقت المزيد من التعرض للأخطار الافتراضية "الالكترونية"، ودفع ذلك المجتمع الدولي لإعادة التفكير في قضايا العلاقة بين الأمن والتكنولوجيا وخاصة بعد أحداث الحادي عشر من سبتمبر٢٠٠١، وأصبح هناك تنام لظاهرة الإرهاب الالكتروني وفي نفس الوقت عدم مواكبة آليات المواجهة مع النمو السريع في انتشار تكنولوجيا الاتصال والمعلومات وزيادة الاعتماد الدولي عليها في البنية التحتية الكونية للمعلومات، ومحدودية دور المواجهة الأمنية والتقنية والسياسية والقانونية .

وكان لذلك كله تأثير على حجم الظاهرة و في تداعياتها وإشكالياتها وطبيعة التكييف القانوني لها، كما كشف عن تناقض المبادئ القانونية القائمة بدرجة أو بأخرى مع ما فرضته تلك القوة الجديدة من تحديات ، الأمر الذي غدا معه القانون الدولي بحاجة ملحة للتكيف مع ظاهرة الفضاء الالكتروني وما تشتمل علية من أنماط لاستخدام القوة والتي تظهر في ابرز صورها في شكل الإرهاب الالكتروني ، ويختبر ذلك في الوقت نفسه قدرة المجتمع الدولي على المواجهة ، و كما اتخذ جهودا مماثلة في حل اكتشاف الطائرات وبروز ظاهرة المجال الجوي وكذلك في مواجهة الإرهاب البيولوجي والنووي والكيماوي.

ويتمثل الدافع وراء ذلك في حقيقة أن التقدم التكنولوجي لا يمكن أن يسير أو يعمل وحده بمعزل عن تقدم قانوني يواكبه ويحافظ عليه ويكفل حمايته ويضع الحلول لما يطرأ من مشكلات بسبب استخدامه حتى يصبح التقدم التكنولوجي أداة للبناء وأساسا لكل تطور..

**ثانيا: المشكلة البحثية وتساؤلات الدراسة**

أما وقد أصبح للفضاء الالكتروني أهمية إستراتيجية في النظام الدولي نتيجة لدوره في كافة النواحي الاقتصادية والأمنية والسياسية والثقافية والاجتماعية والإعلامية مع تزايد الاعتماد عالميا على تكنولوجيا الاتصال والمعلومات وارتباطها بشبكات الاتصالات الحديثة التي أصبحت مسئولة عن نمو الثروة والاقتصاد وتوافر فرص للنمو الاقتصادي على المستوى المحلي والعالمي.

ومثل الفضاء الالكتروني بدوره بيئة إستراتيجية لنمو وبروز أشكال جديدة من الصراع ترتبط بعصر المعلومات، و محاولة إحكام السيطرة على الفضاء الالكتروني أو العمل على توظيفه للاستخدام غير السلمي من جانب العديد من الفاعلين أو حلبة للتنافس الاقتصادي والسياسي والعسكري والإعلامي، وهذا ما يؤشر لنوع جديد من حروب الفضاء الإلكتروني تفجرها الصراعات السياسية والعسكرية ويكون هدفها مهاجمة البنية التحتية الكونية للمعلومات.

وأصبح لدى كافة الفاعلين داخل مجتمع المعلومات العالمي القدرة والإمكانية على شن تلك الهجمات بما أسهم في إيجاد فوضى في استخدام الفضاء الالكتروني والذي أصبح مجالا لاستخدام شتى أسلحة التدمير السياسي الاقتصادي والمالي والنفسي والإعلامي والعسكري مع بروز استخدام غير مشروع للقوة من قبل الأفراد والجماعات والدول واستخدام أسلحة الفضاء الالكتروني في مجال الحماية والهجوم وتطوير القدرات داخل الفضاء الالكتروني لشن عمليات الهجوم على أنظمة الحاسبات التابعة للدول الأخرى.

وانعكاس ذلك على التهديد بعسكرة الفضاء الالكتروني وجعله جزءا هاما من تكتيكات الحروب على خلاف طبيعته المدنية السلمية، وأهميته في عمل البنية التحتية الكونية للمعلومات، وفي ذات الوقت تعرض الفضاء الالكتروني للثغرات الأمنية في البرمجيات والتي تؤدي إلى انتشار الفيروسات وغيرها، بالإضافة إلى تعرض كابلات الاتصالات والانترنت للخطر سواء أكان في شكل متعمد أو غير متعمد ،و العديد من المخاطر الأخرى التي تعبر عن بروز مجتمع الخطر Risk Society في عصر المعلومات.

ناهيك عن بروز تحديات أمنية وقانونية وسياسية وتقنية وثقافية واجتماعية، و ضعف معدلات الحماية تجاه تلك الأخطار وعدم وجود أطر قانونية واضحة تتحكم وتنظم ظاهرة الفضاء الالكتروني و حقوق وواجبات الدول تجاه تلك الظاهرة المستحدثة في النظام الدولي، والتي تكشف في الوقت ذاته عن دور لقوة جديدة ذات طابع لين يمكن أن يطلق عليها "القوة "الالكترونية " والتي أصبحت تستخدم على نطاق واسع وممتد بامتداد الفضاء الالكتروني استخداما غير سلمي تعبيرا عن حالة الصراع من قبل شتى الفاعلين.

وما ترتب على ذلك من بروز قضية الأمن الالكتروني كقضية عالمية تمثل إحدى أولويات الأجندة الدولية بل وظهرت مفاهيم أخرى جديدة للحرب والعدوان والنزاع المسلح والهجوم والإرهاب لم يتم

تضمينها في الاتفاقيات والمواثيق الدولية الحالية مع كل ذلك لا يوجد ثمة تكييف قانوني واضح للمفاهيم والإشكاليات والتداعيات المترتبة على والمرتبطة بالإرهاب الالكتروني على استخدام القوة في العلاقات الدولية ، ومن ثم يمكن القول أن النظام الدولي قد أصبح أمام ظاهرة متعددة الأبعاد ونطاق التأثير والملامح هي ظاهرة الإرهاب الالكتروني المعقدة، والتي تنطوي على كثير من الصعوبات والتحديات التي تتعلق بمدى إمكانية إدراج استخدام القوة بصورتها المرنة داخل الفضاء الالكتروني في الاظار القانوني الذي يتعامل مع استخدام القوة " الصلبة" في العلاقات الدولية، وما ورد في ميثاق الأمم المتحدة في المادة ( ٢ ) فقرة ٤ وشروطه الموضوعة في المادة (٥١) في ميثاق الأمم المتحدة ومدى انعكاس التحول في طبيعة القوة على التكييف القانوني لاستخدامها في الفضاء الالكتروني وما يمثله ذلك من تحديات جسيمة للأمن والسلم الدوليين. ومدى احتياج ذلك لجهد متواصل لإرساء مبادئ جديدة أو تطوير قائمة أو تضمين تلك التحديات في الإطار العام للقانون الدولي لكي تحاول أن تحكم حركة التفاعلات داخل الظاهرة التكنولوجية المتمثلة في الفضاء الالكتروني.

وكل ذلك مما يجعل المشكلة البحثية للدراسة تتلخص في التساؤل الرئيسي :

**ماهية تأثير الإرهاب الالكتروني على استخدام القوة في العلاقات الدولية وعلى الطابع السلمي للفضاء الالكتروني خاصة بعد أحداث ١١ سبتمبر ٢٠٠١؟**

**ويتفرع عن هذا التساؤل عدة تساؤلات فرعية تدور حول:**

١- ما هو الفضاء الالكتروني وخصائصه ؟ ومدى أهميته للمجتمع الدولي ؟ و دوره في التفاعلات السياسية و تغير علاقات القوة والأمن داخل النظام الدولي ؟

٢- ما المقصود بمفهوم الإرهاب الالكتروني وما الذي يميزه عن المفاهيم الأخرى ؟ وما هي خصائصه وأشكاله ؟ وما هي آلياته وأدواته ؟ وهل تعد هجمات الفضاء الالكتروني حرباً أم إرهاباً ؟

٣- كيف تطور الإرهاب الالكتروني ؟ وما هي طبيعة التحديات التي يمثلها للمجتمع الدولي ؟ وهل يمثل شكلاً جديداً من أشكال الصراع الدولي ؟ وهل تعد نمط جديد من استخدام القوة وهل تعد مصدر جديد من مصادر تهديد الأمن الدولي ؟

٤- كيف تعاملت الأطر القانونية الدولية الحالية مع ظاهرة الإرهاب الالكتروني ؟و إلى أي مدى يوجد ثمة فراغ قانوني في التعامل مع الفضاء الالكتروني وكيف السبيل إلى سد هذه الفجوة؟ وهل تعد هجمات الإرهاب الالكتروني استخداما للقوة وهجوما مسلحا وفق القانون الدولي ؟

٥- ما مدى مشروعية استخدام هجمات الفضاء الالكتروني في حالة النزاع المسلح أو الدفاع الشرعي في ظل القانون الدولي الإنساني ؟وهل يمكن تطبيق مبدأ حظر استخدام القوة في العلاقات الدولية الذي يتعلق بالقوة الصلبة على ذلك النمط الجديد من القوة الالكترونية ذات الطابع المرن؟

٦- وكيف يمكن الاستفادة من العرف والقياس كمصادر للقانون الدولي لوضع تكييف قانوني لظاهرة الإرهاب الالكتروني وما مدى الاستفادة من القانون الدولي لحقوق الإنسان وقانون الفضاء الخارجي وقانون البحار في هذا الخصوص ؟

٧- إلى أي مدى يمكن اعتبار الفضاء الالكتروني مرفقاً دولياً وتراثاً مشتركاً للإنسانية ؟ وكيف يمكن تطوير خريطة طريق دولية لتحقيق الأمن الالكتروني العالمي ؟ وما هو الدور الذي يمكن أن تلعبه الأمم المتحدة والمنظمات الدولية في ذلك ؟

## ثالثا: الإطار الزمني للدراسة

يتناول الباحث دراسة ضمن فترة زمنية تبدأ من عام ٢٠٠١حتى فترة انتهاء الدراسة ٢٠٠٧، وذلك لعدد من الاعتبارات والأسانيد التي يمكن تلخيصها كالتالي:

- اما عن تحديد بداية الدراسة بعام ٢٠٠١ قد يرجع ذلك الى عدد من الأسباب تتمثل:

أولاً : شهد ذلك العام أكبر هجوم الكتروني عبر الفضاء الالكتروني في العالم من خلال نشر فيروسات نيميدا Numda والكود رد The Code Red والتي انتشرت بشكل هائل عالميا حيث تأثر ما يقرب من مليون كمبيوتر.

وثانيا : مثل عام ٢٠٠١ بداية الانتشار المتصاعد عالميا لتكنولوجيا الاتصال والمعلومات وزيادة الاعتماد الدولي عليها في البنية التحتية الكونية للمعلومات كما زادت الأهمية الإستراتيجية للفضاء الالكتروني للمجتمع الدولي بتعلقه بكافة المرافق الحيوية في المال والاقتصاد والتجارة والسياسة والإعلام.

وشكلت تلك المتغيرات التكنولوجية تحديا للقانون الدولي سواء بالموقف من الإرهاب الدولي بصفة عامة أو ما يتعلق بإمكانية استخدام الفضاء الالكتروني كأداة أو وسيط في النزاع المسلح أو الإرهاب والصراع، وجاءت تلك الأخطار لتهدد الاستخدام المدني السلمي للفضاء الالكتروني مع غياب استراتيجيات دولية واضحة للمواجهة.

وثالثا : بروز أول اتفاق دولي يعكس بداية الإدراك الدولي بخطر تهديدات أمن الفضاء الالكتروني والذي تمثل في توقيع الاتفاقية الأوروبية للجريمة الالكترونية في نوفمبر٢٠٠١ وما كان لها من دور في دعم الجهود الدولية في مواجهه أخطار الفضاء الالكتروني.

ورابعا : شهد هذا العام أحداث الحادي عشر من سبتمبر، تلك الأحداث التي عكست قدرة تنظيم القاعدة على شن هجمات باستخدام الطائرات المدنية لتدمير برجا التجارة العالمي ومبني البنتاجون ومستهدفا البيت الأبيض وما عكس ذلك من القدرة على توظيف تكنولوجيا الاتصال والمعلومات وآليات العولمة في التخطيط والتنفيذ، وليشهد الفضاء الالكتروني ساحة أخرى للصراع ما بين تنظيم القاعدة والولايات المتحدة، ومثل الإرهاب الالكتروني احد تلك الاستخدامات وطرح ذلك الحدث عده إشكاليات تتعلق الأولى باستخدام الوسائل المدنية كأداة إرهابية وإمكانية استخدام الفضاء الالكتروني في العمل العسكري أو الإرهابي وما يتعلق بدوره في البنية التحتية الكونية للمعلومات .

وتتعلق الإشكالية الثانية باستخدام تنظيم القاعدة لكافة الوسائل التكنولوجية الحديثة في التنفيذ والتخطيط وتعبئة قدراته في التوظيف العسكري للفضاء الالكتروني، أما الإشكالية الثالثة تتجلى فيما طرحته الحملة الأمريكية على الإرهاب والضربات الوقائية مشكلة انتقال ساحة المواجهة بين الولايات المتحدة وتنظيم القاعدة من الفضاء الواقعي إلى الفضاء الالكتروني ليبرز تحوله إلى ساحة للصراع الدولي، وتعلقت الإشكالية الرابعة بالمواجهة الأمنية على مستوى العالم مع تنظيم القاعدة والتي انتقلت إلى الفضاء الالكتروني في شكل تجسس وحجب مواقع وانتهاك خصوصية مسألة الحريات المدنية وحرية التعبير عبر الانترنت كأحد مرتكزات حقوق الإنسان في مواجهه الاعتبارات الأمنية.

- أما تحديد فترة نهاية الدراسة بعام ٢٠٠٧ ذلك لبروز عدة تطورات هامة تعزز الإطار النظري للدراسة وتشكل حلقة مهمة مة من تطور التهديدات للأمن الالكتروني الدولي وكان ابرز تلك الأحداث،

وأولها: بروز خطر استخدام الدول للفضاء الالكتروني لتحقيق أهداف إستراتيجية عبر حدثين هامين أولهما في شهري مايو وابريل من عام ٢٠٠٧ حيث تم استخدام هجمات الفضاء الالكتروني ضد المؤسسات الحكومية في الدول و بما كشف عن دور للدول في ذلك الصراع حيث تعرضت استونيا إلى هجمات استهدفت شل حركة بنياتها التحتية وذلك اثر خلاف سياسي ما بين الأقلية الروسية والحكومة، وأما الحدث الآخر في سبتمبر عام ٢٠٠٧ حيث اتهمت الصين بأنها تقف وراء هجمات عبر اختراق أجهزة الكمبيوتر الخاصة بوزارة الدفاع الأمريكية، كما اتهمت بالمسئولية عن هجمات مماثلة على ألمانيا وفرنسا وبريطانيا ونيوزيلندا، وتعلن الصين من جانبها أنها تقع هي الأخرى ضحية للهجمات،

و ثانيا: تحولت الحرب الافتراضية إلى حقيقة إستراتيجية، ففي عام ٢٠٠٧ أعلن سلاح الجو الأمريكي عن تشكيل "قياده في العالم الالكتروني " لمواجهة هجمات محتملة قد تستهدف تجهيزاته ومعداته المعلوماتية وأنظمته في الاتصالات وذلك من اجل تدريب وتجهيز قوات ضمن سلاح الجو لشن عمليات في الفضاء الالكتروني تكمل العمليات الجوية في الفضاء، واتجهت الولايات المتحدة لتطوير أسلحة هجومية وبدا الاهتمام الدولي يتصاعد مع خطر شن تلك الحرب الجديدة.

وثالثا: أطلق الاتحاد الدولي للاتصالات مبادرته الإستراتيجية للأمن الالكتروني عام ٢٠٠٧ والتي شكلت إطارا مهما للتعاون الدولي في مواجهه أخطار الفضاء الالكتروني والعمل على تعزيز أمن البنية التحتية الكونية للمعلومات. ورابعا: حدوث حالة وعي عالمي متزايد بالاستخدام السيئ للفضاء الالكتروني واتجاه العديد من الدول لسن قوانين محلية لمواجهته مع زيادة الاعتماد الدولي على الفضاء الالكتروني في شتى مجالات الحياة.

## رابعا: أهمية الدراسة

تنبع أهمية الدراسة من كونها – على حد علم الباحث - أول دراسة عربية تتناول بالتحديد أثر الإرهاب الالكتروني على الأمن الدولي و موقف القانون الدولي من تلك الظاهرة كأحد التحديات الأمنية الجديدة، كما ان دراسة الإرهاب الالكتروني تقع ضمن مجال دراسات الصراع الالكتروني

cyber conflict studies التي تتميز بحداثتها عالميا وارتباطها بتكنولوجيا الاتصال والمعلومات القطاع الأكثر نموا وحيوية في الاقتصاد العالمي.

وتكتسب هذه الدراسة أهمية علمية وأخرى عملية يتعلق مضمونها :

## - الأهمية العلمية:

١. إثراء الحوار الأكاديمي حول الإرهاب الإلكتروني ومحاولة للكشف عن القضايا الإستراتيجية التي تتعلق بخطر الصراع الالكتروني، والعمل على استجلاء حقيقة التعقيدات الإستراتيجية التي يفرضها.

٢. بلورة المفاهيم والمقولات المتصلة بأسس الإرهاب الالكتروني في إطار ما يتسم به الإرهاب كمفهوم من عدم وضوح مدلولاته واستخداماته وتشابكه مع غيره من المصطلحات .

٣. تبرز الدراسة الفجوة الفكرية بين ما فرضته هجمات الإرهاب الالكتروني من تحديات وبين الأطر القانونية الدولية الحالية ، ومحاولة سد هذه الفجوة ، وأهمية وجود إسهام قانوني دولي يتناول الظاهرة بأبعادها المختلفة

٤. معرفة موقف الأطر القانونية الدولية الحالية من هجمات الإرهاب الالكتروني والعمل على سد الفجوة التشريعية بينهما ومحاولة الاستفادة مما اقرتة المبادئ والمواثيق الدولية والعرف والقياس كمصادر للقانون الدولي.

٥. محاولة وضع صياغة جادة لمفهوم الأمن الإلكتروني كشكل جديد من أشكال الأمن الدولي في إطار أهمية وجود إطار قانوني دولي حاكم للفضاء الالكتروني باعتبارها ظاهرة حديثة في العلاقات الدولية

٦. معرفة الإشكاليات النظرية وفرص المواجهة والتي تؤثر على الأمن والاستقرار الدوليين، والعمل على رفع الوعي العام والثقافة العالمية الخاصة بالأمن الالكتروني

٧. كما تعد الدراسة محاولة جادة لترسيخ دراسات الصراع الالكتروني والمساهمة في تطوير مفهوم الأمن الإنساني باعتبار أن الإرهاب الإلكتروني يمثل تحدياً للبنية التحتية الكونية للمعلومات.

٨. دفع الخطى الحثيثة لتطوير الجهود الدولية للتقدم في مجال بحث تلك الظاهرة ودراستها ودعم التوجه إلى اتفاقية دولية لأمن الفضاء الإلكتروني .

## - الأهمية العملية:

تكتسب الدراسة أهمية عملية من عدة اعتبارات لعل أهمها :

١. تبرز الدراسة أهمية الفضاء الالكتروني في عمل البنية التحتية الكونية للمعلومات، وكونه عاملا هاما في عمل المرافق الحيوية وأداء الحكومات الالكترونية بالإضافة إلى الاقتصاد الرقمي الجديد و أهميته لحركه النمو الاقتصادي العالمي.

٢. الحث على ضرورة توافر الحماية اللازمة للبنية التحتية الكونية للمعلومات عن طريق برامج الحماية الالكترونية والمادية ، وبلورة فكرة متطلبات وشروط لازمة لإقامة نظام أمني دولي يتعلق بالأمن الالكتروني، وخاصة ما يتعلق بشروط النشأة وشروط الفاعلية.

٣. العمل على تحديد الخطوات لبناء خطة تعاون على المستوى المحلي والدولي لمواجهة الأخطار التي تهدد الفضاء الالكتروني، والإشارة إلى خطورة التصاعد الكمي للإرهاب الالكتروني مع الزيادة المستمرة في انتشار تكنولوجيا الاتصال والمعلومات عالمياً

٤. العمل على تنسيق الجهود الدولية من خلال المنظمات المعنية والأمم المتحدة لإنشاء سياسة أمنية تضع الإرهاب الالكتروني وأخطار الفضاء الالكتروني الأخرى ضمن أولوياتها وأجندتها الأمنية

٥. والعمل على تحسين الجاهزية الدولية لمواجهه أخطار الفضاء الالكتروني وحث المجتمع الدولي لتطوير خطة عمل و اتخاذ خطوات عملية لدعم الأمن الالكتروني ولفت انتباه صانعي القرار وواضعي التشريعات بدول العالم إلى ضرورة العمل على مواجهة ما قد يسببه الإرهاب الالكتروني من أخطار مادية ومعنوية ،

٦. إلقاء الضوء على الطابع الدولي العابر للحدود للإرهاب الالكتروني الذي يجعل الإنسانية محلاً للاعتداء وليست بالضرورة أفرادا أو دولا

٧. محاولة تحديد الموقف من إمكانية تطبيق مبدأ حظر استخدام القوة في العلاقات الدولية على هجمات الإرهاب الالكتروني كنوع جديد من ممارسة القوة ومشروعية استخدامها في حالة النزاع المسلح أو الدفاع الشرعي.

٨. وأخيرا تعمل الدراسة على توفير مادة علمية عن الإرهاب الالكتروني لتصلح لتكون قاعدة بيانات تخدم صانعي القرار والحكومات والشركات العاملة في مجال تكنولوجيا الاتصال والمعلومات والقطاع الخاص والأجهزة الأمنية والأكاديميين والباحثين والصحفيين وغيرهم.

## خامسا :أهداف الدراسة

١. معرفة ماهية الفضاء الالكتروني وخصائصه واهميتة للمجتمع الدولي وطبيعة دوره في تغير علاقات الأمن والقوة وإحداث التغييرات السياسية والاقتصادية والاجتماعية داخل النظام الدولي.

٢. التعرف على ماهية مفهوم الإرهاب الالكتروني وإشكاليات تعريفه وآلياته وتطوره وعلاقته مع غيره من المفاهيم المرتبطة وطبيعة توصيف هجمات الفضاء الالكتروني.

٣. معرفة كيف تطور الإرهاب الالكتروني وطبيعة التحديات التي يمثلها للمجتمع الدولي، والوقوف حول إمكانية اعتبارة شكل جديد من أشكال الصراع الدولي وإضافة أنماط جديدة لاستخدام القوة في العلاقات الدولية

٤. معرفة موقف الأطر القانونية الدولية الحالية من هجمات الإرهاب الالكتروني والعمل على سد الفجوة التشريعية بينهما ومحاولة الاستفادة مما اقرتة المبادئ والمواثيق الدولية والعرف والقياس كمصادر للقانون الدولي.

٥. محاولة تحديد الموقف من إمكانية تطبيق مبدأ حظر استخدام القوة في العلاقات الدولية على هجمات الإرهاب الالكتروني كنوع جديد من ممارسة القوة ومشروعية استخدامها في حالة النزاع المسلح أو الدفاع الشرعي.

٦. المساهمة في تطوير مفهوم الأمن الإنساني الشامل باعتبار أن الإرهاب الالكتروني يمثل تحديا للبنية التحتية الكونية للمعلومات

٧. أهمية دور الأمم المتحدة والمنظمات الدولية في دفع الجهود الدولية لتوفير أساس الأمن الالكتروني الدولي، والعمل على وضع إطار قانوني دولي حاكم له.

٨. دعم التوجه للتوصل لاتفاقية دولية حول الأمن الالكتروني، والعمل على الوصول إلى معايير للأمن الالكتروني على مستوى العالم، وأهمية تحقيق التعاون ما بين كافة الفاعلين داخل مجتمع المعلومات العالمي.

## سادسا : الدراسات السابقة

كانت بداية استخدام هذه الكلمة "الإرهاب الالكتروني" cyber terrorism في فترة الثمانينيات في دراسة "باري كولن Barry Collin "والذي خلص فيها إلى صعوبة تعريف ظاهرة الإرهاب التكنولوجي بدقة ، ناهيك عن الأساليب والحلول المطلوبة لمواجهته وكذلك تحديد دور الكمبيوتر والانترنت في العمل الإرهابي، ولكن اقتصر تناول ذلك المصطلح للإشارة إلى تلك الهجمات التي يستخدم فيها الكمبيوتر ضد اقتصاد وحكومة الولايات المتحدة، ثم اتسع هذا المفهوم مع بداية التسعينات التي شهدت حدوث نمو متزايد للانترنت واستخدامه كما ظهر الجدل حول ظهور مجتمع المعلومات عالميا، إلى جانب الدراسات العديدة التي تناولت المخاطر المحتملة التي تواجهها الدول الغربية خاصة الولايات المتحدة في اعتمادها الكبير على التكنولوجيا وأجهزة الكمبيوتر، وفي تلك الفترة أي في بداية التسعينات صدر تقرير عن الأكاديمية الوطنية الأمريكية للعلوم عن أمن الكمبيوتر حذر فيه من تعرض الولايات المتحدة لبيرل هاربور الكتروني جديد ".

وجاءت أحداث ١١ سبتمبر ٢٠٠١ لتشكل نقلة نوعية كبيرة في الاهتمام بالإرهاب الالكتروني سواء من جانب الولايات المتحدة أو في العالم والذي اتخذ في بدايته بعدا سياسيا بالتركيز على الظاهرة باعتباره ضمن اهتمامات الأمن القومي وأمن الفضاء المعلوماتي، وانتقلت القضية بعد ذلك لتتعدى العامل السياسي لتأخذ بعدا اقتصاديا حيث الصناعة الكاملة حول الأمن المعلوماتي وتأثيرات ذلك على الاقتصاد الرقمي الجديد التي يشكل قاطرة النمو الاقتصادي في الدول المتقدمة، إلى جانب الصناعات التي من الممكن أن تتعرض لتلك المخاطر لينتج عنها خسائر محتمله في الاقتصاد والأرواح، وتقع الأخطار التي تنجم عن استخدام الفضاء الالكتروني في مفترق طرق من الاهتمام من كافة الباحثين والأكاديميين.

ويأتي هذا مع ظهور علم جديد و دراسات حديثة في الاهتمام الدولي تعبر عن شكل جديد من الصراع الذي ارتبط بظاهرة الفضاء الالكتروني كنطاق جديد في العلاقات الدولية و يرتبط بصراعات عصر المعلومات، إلا وهي دراسات الصراع الالكتروني وهي تلك الدراسات التي تميزت بالتنوع والتعدد وذلك وفقا لوجهه النظر التي يتبناها الباحث أو وفق المجال أو التخصص الذي ظهر في التنوع الكبير لدراسات تتناول الفضاء الالكتروني ضمن وسائل الإعلام الجديد ونظريات الاتصال، ودراسات أخرى تعنى به في إطار الصراع في السياسية الدولية وهناك أيضا دراسات عملت على دراسة الإرهاب الالكتروني ضمن الجريمة الالكترونية.

وهناك دراسات أخرى ركزت على جانب واحد من أحد المتخصصين في مجال محدد، وانعكس ذلك على اختلاف درجات الاهتمام والتخصص من جانب الدارسين والباحثين، فهناك دراسات خاصة بعلوم الكمبيوتر وامن الانترنت والشبكات، و دراسات خاصة بالطابع العسكري والدفاعي في إطار التوظيف العسكري للفضاء الالكتروني.

وحظي الإرهاب الالكتروني باهتمام خبراء الإرهاب والعلوم الاجتماعية وعلم النفس والعلاقات الدولية والقانون الدولي والتعليم والفلسفة كما إن هناك دراسات تناولت ذلك الصراع من وجهة نظر اقتصادية، ويرجع هذا التنوع من الاهتمام لشمول تلك الدراسات محور التفاعل ما بين الإنسان والكمبيوتر، والاستخدام السياسي لوسائل تكنولوجيا الاتصال والمعلومات والطابع العالمي للعلوم الإنسانية بصفة عامة، وانعكس ذلك على تنوع درجات ومستويات الاهتمام من جانب كافة المهتمين، وظهر ذلك في تنوع القضايا وأجندات البحث والمرجعيات الفكرية التي تراوحت ما بين التركيز على القضايا التكنولوجية والأخرى ذات الطبيعة الإستراتيجية.

وانعكس الجدل حول مفهوم الإرهاب في الأدبيات العلمية على تناول قضية الإرهاب الالكتروني التي قد تشترك مع الإرهاب التقليدي في الدوافع والأهداف والأبعاد السياسية، ولكنها اختلفت في الخصائص والتداعيات والوسائل وسبل المواجهة خاصة مع وجود فراغ تشريعي وقانوني دولي في تناول تلك الظاهرة، ويمكن الإشارة إلى أهم تلك الدراسات وفق ما يلي :

- <u>دراسات تهتم بالإرهاب الالكتروني ضمن دراسات الأمن الدولي:</u>

وهي تتشابه مع الدراسات الخاصة بالأسلحة النووية ويتم التركيز على حرب الفضاء الالكتروني cyber warfare، وما يتعلق بها من تساؤلات حول التنظيمات الرئيسية والقدرات الخاصة بالاستخدام والأبعاد الفنية والاقتصادية للهجمات الالكترونية والمشاكل التي تواجهها، وتأثير الفضاء الالكتروني على الخصوصية والرقابة وعلى عمل البنية التحتية الحرجة والقابلية للخطر مع الاعتماد الدولي المتزايد، وهناك من رأى في الإرهاب الالكتروني جزءاً من التداعيات الأمنية للعولمة وعصر المعلومات كدراسة "كاسيا وشرواسكا" Kasia Wichrowska "بعنوان "التقدم في تكنولوجيا المعلومات و عولمة الأمن الدولي، و دراسة "لين اي دافيس" Lynn E.Davis "بعنوان "التداعيات الأمنية للعولمة، وأيضا دراسة "سي

بي تي أوي كيم مينج "CPT Ow Kim Meng" بعنوان "الإرهاب الالكتروني :بزوغ الخطر الأمني للألفية الجديدة ".[1]

- هناك دراسات تتعلق بالمشروعية القانونية

تركز على رؤية هجمات الإرهاب الالكتروني من زاوية الشرعية القانونية والأخلاقية وعلاقة ذلك بقانون الحرب والقانون الدولي لحقوق الإنسان والقانون الجنائي، وأثر الفضاء الالكتروني في طبيعة العلاقات المدنية العسكرية وإمكانيات حرب الفضاء الالكتروني والتي يكون لها تأثير على الصراع، أو ما يتعلق بمسالة تقييم تلك الهجمات وفقا للاتفاقيات الدولية والثنائية والإقليمية والعمل على بث الثقة وتقوية آليات المواجهة. دراسة لـ " ميشيل ن. شميت Michael N. Schmitt بعنوان "حرب الشبكات: الكمبيوتر كأداة للقتال وقانون الحرب "تناول فيها موقف قانون الحرب من هجمات الكمبيوتر إمكانية القيام بمثل تلك الاعتداءات كأداة من أدوات النزاع المسلح الدولي, ويمكن أن تكون عواقبها بعيدة المدى.[2] وهناك من تناول إمكانية تطبيق البرتوكولين الإضافيين لاتفاقية جنيف على هجمات الكمبيوتر مثل " دراسة" كونت دورمان Knut Dormann" والتي تحدثت عن إمكانية وجود حظر على استخدام هجمات الكمبيوتر وحماية المدنيين وقت النزاع المسلح.[3]

- دراسات تنظر إلى الإرهاب الالكتروني كقضية عسكرية:

وتتعلق بسيناريوهات الهجوم والدفاع وما يرتبط بها من نماذج المحاكاة والتدريب واختبار مراكز القيادة والسيطرة وطرق تطوير وسائل فعالة لقياس إمكانيات وقدرات أسلحة حرب الفضاء الالكتروني وتحديد الفاعلين وما يتعلق بدور التعاون الدولي.ففي كتاب لـ هايدي والفين توفلر، Heidi& Tofflerعن "الحرب والحرب المضادة "، [4] أشارا إلى أن الطرق التي نعبر بها عن صراعاتنا إن هي إلا انعكاس لمجتمعنا، وان تلك الطرق تعكس أيضا الفترة التاريخية وبيئة الصراع، وقاموا بتقسيم التاريخ البشري إلى ثلاث موجات صراعيه الأولى هي الموجه الزراعية والثانية الموجه الصناعية والثالثة هي الموجة المعلوماتية الجارية؛ ففي الموجه الزراعية كانت عملية الصراع تعكس القدرة والسيطرة على الموارد الطبيعية، وعكست الموجه الصناعية فترة وأسس وسائل الإنتاج، أما الموجه الثالثة والتي تتمثل في الموجه المعلوماتية حيث تم استبدال وسائل الإنتاج بوحدات الإنتاج والتخصص حيث شجع على تنويع الموارد والبشر، وأصبح الاعتماد على التكنولوجيا والمعلومات والاتصال المتبادل لتحقيق التخصصية

---

(1) CPT Ow Kim Meng, **Cyber-Terrorism: An Emerging Security Threat Of The New Millennium** , POINTER, the official journal of the Singapore Armed Forces, V28 N3, Jul - Sep 2002

(2) Michael N Schmitt " Wired warfare: Computer network attack and jus in bello , RICR Juin IRRC June, Vol. 84 No 846, 2002

(3) Knut Dörmann," Computer network attack and international humanitarian law", The Cambridge Review of International Affairs "Internet and State Security Forum", , Trinity College, Cambridge, UK,19 May 2001,and also ,
Dimitrios Delibasis, State Use of Force in Cyberspace for Self-Defence:A New Challenge for a New Century , Peace Conflict and Development: An Interdisciplinary Journal, Issue 8, February 2006,
Duncan B. Hollis," Why States Need an International Law for Information Operations ", Lewis & Clark Law Review, Vol. 11, p. 1023, 2007

(4) Alvin and Heidi Toffler " Forword:the new intangibles ", in Athena s camp: preparing for conflict in the information age ", edited by john arquilla & David ronfeldt ", Santa monica,ca:rand,1997

المعلوماتية، وأصبحت تلك الطريقة ترتبط بالجيوش بما اثر على أدائها وقدراتها وفي اطار ما يعرف بالثورة في الشئون العسكرية. [1]

■ دراسات تنظر للإرهاب الالكتروني كتعبير عن أجندة جديدة للأمن الدولي:

حيث يتم التركيز على المزايا والعيوب ودور الفاعلين من غير الدول في تنمية قدراتهم في استخدام قدرات التحكم في الفضاء الالكتروني واثر ذلك على طبيعة على طبيعة الأزمة وإدارتها ومداولات الحرب الجديدة، وكيف يمكن أن يكون لتكنولوجيا الاتصال والمعلومات دور في دعم السلام والدبلوماسية والمصالحة من خلال الفضاء الالكتروني، وأيضا دور الفضاء الالكتروني في دعم وتطوير أسلحة الدمار الشامل كالأسلحة البيولوجية أو النووية أو النانو تكنولوجي.

وهناك من تناول تلك الظاهرة في إطار الدراسات السلوكية حيث يتم الاهتمام بأثر البيئة على السلوك الإنساني.وهناك بعض الدراسات التي تناولت الإرهاب الالكتروني ضمن الأنواع الأخرى المرتبطة به في محاولة لتمييزه عنها كالجريمة الالكترونية وحرب المعلومات ونشطاء الانترنت كالدراسة التي حررها كل من جون ارقويلا " John Arquilla "و دافيد رونفيلدت، "David Ronfeldt"بعنوان"مستقبل الإرهاب والجريمة والعسكرة، [2] ودراسة "دروثي إ. دينينج" .Dorothy E- Denningبعنوان "نشطاء الانترنت والقراصنة والإرهاب الالكتروني: الانترنت كأداة للتأثير في السياسة الخارجية "، [3]

■ دراسات تنظر للإرهاب الالكتروني على انه شكل من أشكال الحرب غير التقليدية:

وتناولت بعض الدراسات الأخرى هذا النوع ضمن مفهوم الحرب غير التقليدية وكان أول من استخدم مفهوم الحرب غير التقليدية Unrestricted Warfare جنرالان من الصين هما Qiao Liang & Wang Xiangsui في كتابهما الصادر عام ١٩٩٩، وجذب هذا المفهوم أيضا اهتمام "جون هوبكينز" Johns Hopkins . لتنتهي تلك الجهود إلى اعتبار الأسلحة النووية والكيماوية والبيولوجية من ضمن أشكال الحرب التقليدية، وقام "كيفين كولمان Kevin Coleman"في دراسته بعنوان "تحديات الحرب غير التقليدية نظرة للأمام ونظرة للخلف " [4]بتحديد ١٤ نوعا من الحروب غير التقليدية كان هناك مالا يقل عن ستة أنواع ترتبط ارتباطا مباشرا بالإرهاب الالكتروني وهي حرب المعلومات والحرب الإعلامية وحرب الشبكات والاتصالات والحرب السياسية والحرب السيكولوجية والحرب التكنولوجية وبالطبع الإرهاب، في حين يرتبط الإرهاب الالكتروني بالأنواع الأخرى بطريقة غير مباشرة.

---

(1) David J. Lonsdale, **the Nature of War in the Information Age: Clausewitzian Future.** New York, Frank Cass, 2004.

(2) John Arquilla and David F. Ronfeldt. Cyber war is coming. Santa Monica, CA: Rand, 1992.

_______________,Networks and Netwars: The Future of Terror, Crime, and Militancy, RAND, 2001

(3) Dorothy Denning & Elizabeth Robling. **Information Warfare and** Security. New York, ACM Press, 1999. Dorothy Denning, "Information Warfare and Cyber-terrorism," Women in International Security (WIIS) Seminar, Washington, D.C. (15 December 1999

(4)Kevin Coleman , The Challenge of Unrestricted Warfare - A Look Back and a Look Ahead.Articles , www.directionsmag.com, Jan 11, 2006,

وقام كولمان بتطبيق معايير كمية على هذا النوع الجديد من الصراع حيث ربط بين الإرهاب الالكتروني والحرب الالكترونية والحرب غير التقليدية ، وأكد أنها مرشحه للزيادة في غضون السنوات القادمة، وقد قام" كيفين كولمان" Kevin Coleman بعمل مصفوفة عبر فيها عن تحليل كمي للخطر يتراوح من الدرجة (1) إلى الدرجة (5) من خطر منخفض إلى خطر مرتفع ومستندا على دراسة الدوافع والإمكانيات لكل خطر من أخطار الحرب غير التقليدية، وقام بتقسيمها إلى الخطر الحالي والخطر المتوقع في المدى القصير وفي المدى الطويل وتداعياتها في الوقت الحالي والمدى القصير والطويل وكذلك قام بقياس القدرة على الدفاع ضد تلك الأخطار ودرجة التغير في الخطر.(1) ، ويؤخذ على تلك الدراسات صعوبة التحليل الكمي ووجود عوامل لا يمكن أن تخضع للقياس كالأفكار التي تحرك هذا الإرهاب أو تلك القوة.

- دراسات ركزت على الارهاب الالكتروني كنمط جديد من الصراع الالكتروني

كما أن دراسة الإرهاب الالكتروني تقع ضمن مجال دراسات الصراع الالكتروني cyber conflict studies مثل دراسة Athina Karatzogianni والذي أوضح كيف ان للصراع الجديد عبر الفضاء الالكتروني من تأثير على السياسة الدولية (2) وكذلك هناك دراسات ركزت على كيفية تحول الصراع إلى الطابع الالكتروني مثل دراسةBonnie N. Adkins واوضح أيضاً تطور ذلك الصراع من مجرد القرصنة الى حرب المعلومات وغيرها من الأشكال المتطورة للحرب (3) وقدم James Mulvenon شرحا وافيا لطبيعة الصراع الالكتروني (4) ومحاولا إرساء نمط جديد من الدراسات التي تتعلق بالصراع .

- دراسات ركزت على استخدام الجماعات الإرهابية للإرهاب الالكتروني :

حيث تتناول كيفية استخدام المنظمات الإرهابية للانترنت كدراسة جبرائيل ويمانGabriel"Weimann" كيف يستخدم الإرهاب الحديث الانترنت "وعرض من خلالها كيفية استخدام المنظمات الإرهابية للانترنت وأنواع ذلك الاستخدام كما أكد "ويمان"على خطر الإرهاب الالكتروني في دراسته اللاحقة بعنوان "الإرهاب الالكتروني كيف يصبح خطرا حقيقيا على الانترنت"، و أيضا في كتاب "ويمان" الصادر في ابريل ٢٠٠٦بعنوان "الإرهاب على الانترنت ".(5)

وهناك من تناول الإرهاب الالكتروني كتطور في وسائل التخطيط للعمل الإرهابي كالدراسة التي تناولت العلاقة بين التكنولوجيا والإرهاب والتي صدرت عام ١٩٩٨بعنوان "التكنولوجيا والإرهاب:التهديد الجديد للألفية الجديدة "كتبها "استيفن ارياورز وكمبرلي اركيز"حيث أقرت

---

(1) Kevin G. Coleman, **The world war 111,A Cyber War has begun, Cyber Warfare, The Technolytics Institute**, September 2007(http://www.technolytics.com/Technolytics_Cyber_War.pdf)

(2) Athina Karatzogianni,(ed), "Cyber-Conflict and Global Politics"', Routledge and Taylor & Francis Group. , 11th September 2008

(3) Bonnie N. Adkins, ," **The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?"**, A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, Maxwell Air Force Base, Alabama, April 2001

(4) James Mulvenon ," **Toward a Cyberconflict Studies Research Agenda**",in "On the Horizon",O.sami Saydijari,(editor), IEEE computer security ,july/august 2005

(5) Gabriel Weimann, Terror on the Internet: The New Arena, the New Challenges. Washington, United States Institute of Peace Press, 2006

بإمكانية التنظيمات الإرهابية الحصول على ما تريد من معلومات عبر الاستخدام المقنن للكمبيوتر ومن خلال استغلال الثغرات شبكات المعلومات أو باللجوء لعمليات القرصنة المعلوماتية والدخول إلى شبكات المعلومات العسكرية والأمنية للدول لاستغلالها في التخطيط للعمل الإرهابي وتنفيذه أو الدخول على شبكات البورصة.

ويؤخذ على هذه الدراسات أنها ركزت على استخدام الجماعات الإرهابية كتعبير وحيد عن الإرهاب الالكتروني، كما إنها ارتكزت على دراسة تنظيم القاعدة كمنظمة إرهابية مضافة إليها مواقع الانترنت التي لا تحتوي إلا محتوى ثقافي ديني حيث تم الخلط في هذه الدراسات بين موقع ذي طبيعة دينية وأخرى تحض على الإرهاب والعنف وربما يرجع ذلك إلى فقدان الفهم الواعي للثقافة الإسلامية ومشكلات تتعلق بفهم اللغة العربية وعدم وجود مترجمين جيدين لها. كما ركزت تلك الدراسات الخاصة بالإرهاب الالكتروني على ما تقوم بة الجماعات الإرهابية والتغاضي عن دور الدول التي يمكن أن تقوم هي أيضا بالإرهاب الالكتروني وتم التركيز على الاعتبارات الأمنية فقط .

- وهناك دراسات تعلقت بتناول الموضوع من زاوية الأمن الالكتروني

حيث ركزت الدراسات المتعلقة على زوايا مختلفة للأمن الإلكتروني:

- تم التركيز على الأمن الالكتروني كقضية تتعلق بأمن تكنولوجيا الاتصال والمعلومات مع اهتمام قوي بأمن الفضاء الالكتروني حيث تهدف تلك السياسات إلى احتواء التهديدات للبنية التحتية من خلال الوسائل التقنية مثل حوائط النار أو برامج مكافحة الفيروسات أو منع الاختراق ويكون الفاعلون في هذا المجال المتخصصين في امن تكنولوجيا الاتصال والمعلومات[1]

- الأمن الالكتروني كقضية اقتصادية حيث ينظر إلى الأمن الالكتروني من خلال علاقته بمجتمع الأعمال والاقتصاد وخاصة التجارة الالكترونية، والتي تتطلب الدخول الدائم والآمن للبنية الخاصة بتكنولوجيا الاتصال والمعلومات وبما يشكل عاملا أساسيا في النمو الاقتصادي وفي التأثير الإيجابي على كافة القطاعات ويكون الفاعلين في هذا المجال هم من القطاع الخاص.

- الأمن الالكتروني كقضية قانونية حيث ينظر إلى الأمن الالكتروني من خلال علاقته بمصادر التهديد مثل الجريمة الالكترونية وهو مفهوم واسع يشمل كافة أنواع الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات وارتكاب الجرائم ضد الحاسبات الشخصية والإرهاب الالكتروني وحرب المعلومات ويخضع ذلك لاهتمام رجال القانون.

- الأمن الالكتروني كقضية أمن قومي حيث يصبح المجتمع بصفة عامه معرض للخطر من خلال اعتماده على تكنولوجيا الاتصال والمعلومات ويمكن المواجهة من خلال العديد من المستويات الفنية والتشريعية والتنظيمية والمؤسسات الدولية ويهتم بذلك المتخصصين في الأمن ويتضمن ذلك الأخطار الأساسية التي يمكن أن تصدر من الإرهابيين أو حرب المعلومات التي يتم استغلالها من قبل دول أخرى.

---

[1] Seymour E. Goodman and Herbert S. Lin (eds),"**Toward a Safer and More Secure Cyberspace,** Washington, National Academies Press, 2007.

▪ أما فيما يتعلق بتقدير الخطر الذي يمثله الإرهاب الالكتروني على المجتمع الدولي فقد تنوعت الدراسات السابقة في عدة اتجاهات هي:

الاتجاه الأول:عمل على التضخيم من خطر الإرهاب الالكتروني باعتباره أحد حروب المستقبل ومن ثم عملت على تعظيم عامل الأمن على الحريات الشخصية وحقوق الإنسان واعتباره من ضمن الأخطار غير التقليدية التي تهدد البشرية في العقود القادمة، كدراسة "من السيارات المفخخة إلى القنابل المنطقية نمو الخطر من الإرهاب المعلوماتي " لـ جيرولد م بوست ".Jerrold M Post"

و الاتجاه الثاني، عمل على التقليل من خطره وأن مسألة الترويج لمخاوف الإرهاب الالكتروني يكمن وراءها مصالح الشركات العاملة في تكنولوجيا المعلومات وخاصة ما يتعلق بالأمن الرقمي والتنافس بين تلك الشركات وبعضها البعض، كدراسة "أسطورة الإرهاب الالكتروني The Myth of Cyber terrorism"التي نشرها جوشوا جرين " Joshua Green " في نوفمبر 2002 بدورية Washington monthly وقلل فيها من شأن الإرهاب الالكتروني لصالح الأنواع الأخرى الأكثر فاعليه كوسائل إرهابية.[1]

والاتجاه الثالث: ينظر برؤية موضوعية لذلك الخطر الجديد معتبرا أن ذلك التهديد إن لم يكن محسوسا في الوقت الحاضر فان خطره سيتعاظم في المستقبل، ومن ثم على العالم الاستعداد لتلك المرحلة كدراسة "مارك م بولليت "Mark M. Pollitt عن "الإرهاب الالكتروني حقيقة أم خيال".

## سابعا: الإطار المفاهيمي للدراسة:

ركز الباحث على بعض المفاهيم الحاكمة والرئيسية للدراسة يتمثل أهمها فيما يلي:

- الفضاء الالكتروني:

كان أو ل استخدام لمفهوم "الفضاء الالكتروني " Cyber space لـ "وليام جيبسون " William Gibson في كتابة الكلاسيكي عام 1984 وجاءت جهود "نيل استيفسون " Niel Stephenson عام ١٩٨٩ ليرسما معا صورة تكاد تكون شاملة عن ماهية ذلك المفهوم والتي تحددت في أنه ذلك الفضاء أو المحتوى والبديل الكوني الذي يمكن من خلاله الناس أن تشارك فيه ووصف"وليام جيبسون " العالم الرقمي بأنه عبارة عن شبكات الكمبيوتر والاتصالات الالكترونية وعبارة عن شبكة كمبيوتر خيالية تحتوي على كم هائل من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة " حيث تقترب العلاقة بين العالم المادي والعالم الواقعي بحيث يحصل مستخدمو الكمبيوتر على خبرات لا وجود لها يكتسبونها عن طريق هذا الاستخدام فتؤثر المكونات الرقمية على العالم المادي والذي يمكن أن نسمعه ونراه ونحسه ونتأثر به ونقرأه. وأصبحت قوة الكمبيوتر والشبكات تتزايد عاما بعد عام لتجعل من السهولة إدراك وجود هذا المكون الالكتروني، وهذا ما جعل الناس يرون في الفضاء الالكتروني على أنه عالم مواز للواقع الذي نعيش فيه و الفضاء الالكتروني شأنه شأن كلمة الفضاء التقليدية حيث يتألف من أربعة مكونات رئيسية هي المكان والمسافة والحجم والمسار ويعبر محتواها عن طبيعة وجود هذا المحتوى ويتميز هذا الفضاء الالكتروني بغياب الحدود الجغرافية وغياب الحكم القاهر لعنصر الزمن.

---

[1] Joshua Green. "The myth of cyber terrorism" ,**Washington monthly** ,November 2002.

- الصراع الالكتروني:

يُعد مفهوم الصراع Conflict هو أحد أبرز المفاهيم المتداولة التي طفت على سطح النقاش المحتدم بعد انتهاء الحرب البادرة، وتأخذ الصراعات شكل تطور المجتمع الدولي حيث تكون تعبيرا عن الواقع الاجتماعي والتكنولوجي، ففي عصر الثورة المعلوماتية يأخذ الصراع أدوات جديدة للتعبير وما ينعكس على تداعياته وأطرافه، ومثل ظهور الفضاء الالكتروني ساحة جديدة إما لنقل الصراعات من خلاله أو استخدامه نفسه كوسيلة من وسائل الصراع والذي يعد امتدادا طبيعيا للصراع بشكله المادي.

ومن ثم فان الصراع الالكتروني هو ذلك الصراع الذي يمكن أن ينشب في بيئة يكون وسيطها الفضاء الالكتروني حيث يشهد حركة التفاعلات بين مختلف أنواع الصراعات والتي قد تنشب من كل أنواع البيئات الأخرى غير المتصلة بالفضاء الالكتروني وإنما تؤثر فيه كالنزاعات بين الإفراد والصراع ذي الطابع القانوني والتجاري أو الصناعي ويمتد ليشمل كافة مجالات الحياة التي يمكن أن تصبح مجالا للصراع والتنافس. ويستخدم الفاعلون الفضاء الالكتروني للتعبئة والحشد والتنظيم والدعاية ويستخدمها أيضا المعارضة ضد النظم السياسية أو نشطاء الإرهاب أو الجريمة، ويمكن للصراع الالكتروني أن يحدث داخل أو عبر كل جهاز عام أو خاص وتمدد داخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول، ويؤثر ذلك في امتداد مجال الصراع ونطاقه وبما يؤثر على تفاقم تداعياته أو أثارة حيث يتم الاستخدام المتعدد للصراع من وجهة نظر الاقتصاد والسياسة والاجتماع أو الأمن أو الثقافة.

- الإرهاب الالكتروني

هو يعبر عن التقاء الإرهاب وعالم الكمبيوتر وأنه الاستخدام غير المشروع للقوة والتهديدات بضرب أجهزة الكمبيوتر والشبكات والمعلومات المختزنة فيها من أجل ترويع وإكراه الحكومات وشعوبها من أجل تحقيق أهداف سياسية واجتماعية، ولكي يعتبر ذلك إرهاب لابد أن يؤدي إلى ترويع وإكراه الحكومات والأشخاص والممتلكات أو على الأقل التسبب في الضرر والخوف، وكذلك إحداث ضحايا وإيذاء بدني وانفجار وأضرار اقتصادية جسيمة والهجوم على البنية الأساسية وإعاقة عمل الخدمات الأساسية ."تعريف "دينيج .د " Denning .D، أو "أنه عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنه عنف وتدمير أو بث الخوف تجاه تلقي الخدمات بما يسبب الارتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة "تعريف وزارة الدفاع الأمريكية".

- الجريمة الالكترونية

تشير الجريمة الالكترونية إلى النشاطات التي يكون لها صفة عدم الشرعية من أطراف معينة والتي يتم ارتكابها عن طريق الشبكات الالكترونية العالمية، وبصفة عامة فإن الجريمة الالكترونية يمكن أن يتم تعريفها على أنها جريمة يتم ارتكابها في بيئة الفضاء الالكتروني والتي تشمل الانترنت وشبكات الكمبيوتر وأنظمة الاتصالات اللاسلكية، ويعد سلوك الجريمة الالكترونية هو عبارة عن انتهاك القانون الجنائي عن طريق استخدام تكنولوجيا الكمبيوتر، وعلى الرغم من وجود عدد من

الالتباسات حول تحديد الجريمة الالكترونية إلا أن هناك اقترابين مختلفين لتحديد ماهية الجريمة الالكترونية، الأول يأخذ في اعتباره دور الكمبيوتر في الجريمة ووفقا لهذا الاتجاه هناك ثلاثة أنماط للجريمة المرتبطة بالكمبيوتر.

حيث يمكن أن يكون الكمبيوتر هدفا للجريمة ويمكن ذلك عن طريق سرقة البرمجيات أو الأجهزة الخاصة بالكمبيوتر، أو أن يخضع الكمبيوتر للجريمة حيث يكون الكمبيوتر وفق هذا التحديد ضحية للجريمة أو يخضع لها، أما النوع الثالث فيتعلق بكون الكمبيوتر يمكن أن يكون أداة لارتكاب الجريمة التقليدية، أما الاتجاه الثاني للتعامل مع الجريمة الالكترونية: فيرى الجريمة الالكترونية من خلال أربعه أنواع، الأول أن الكمبيوتر يكون هدفاً: حيث يتم تعرض الكمبيوتر لعملية منع مستخدميه من الاستفادة من الخدمات وتشمل جرائم من قبيل سرقة المعلومات أو الملكية الفكرية. أما النمط الثاني فان الكمبيوتر يصبح وسيلة للجريمة وهو يقترب من النمط الأول حيث يتم استخدام الكمبيوتر كوسيلة لارتكاب الجريمة التقليدية، أما النمط الثالث أن يكون الكمبيوتر كنمط للجريمة حيث يتم ارتكاب الجريمة عندما يتم استخدامه استخداماً إجراميا ويتم فيه استخدام الكمبيوتر بسهولة لتسهيل تنفيذ العمليات الإجرامية مثل غسيل الأموال، أما النمط الرابع من الجرائم فيرتبط بانتهاك الخصوصية كانتهاكات الطباعة والنسخ للبرمجيات أو سوء استخدام الخدمات الالكترونية وأنظمة الهاتف.

- حرب المعلومات.

تنقسم حرب المعلومات إلى نوعين: نمط هجومي ونمط دفاعي، فالهجومي تقوم به في الغالب الدولة وأجهزة استخباراتها لما تمتلكه من إمكانيات ضخمة تؤهلها للقيام بها، حيث تستخدم حرب المعلومات الهجومية لأهداف سياسية وعسكرية أو لمجرد الإثارة وإظهار القدرات، حيث يستحوذ المهاجم على المعلوماتية ونظمها، ويقوم بالتجسس وسرقة البرامج الحاسوبية، وقد يقوم بتخريب أو تعطيل تنظيم المعلوماتية .أما الحرب الدفاعية :فهي تعمل على الحد والوقاية من أعمال التخريب التي قد تتعرض لها، وتختلف الوسائل الدفاعية باختلاف أدوات التخريب والمعلوماتية وطبيعة الأضرار التي قد تحدثها.

وتستخدم الحرب المعلوماتية لتحقيق أهداف إستراتيجية والتي قد تستخدم لتحقيق أهداف قومية عن طريق التأثير أو السيطرة على كل العناصر(السياسية والاقتصادية والعسكرية والمعلوماتية ) أما على المستوى العملياتي الميداني فإنها تستخدم للتأثير على شبكات الاتصالات والدعم اللوجستي والقيادة والسيطرة وكل الأنشطة والإمكانيات التي يمكن أن تستخدم، وأما على المستوى التكتيكي فهي تهدف إلى التأثير على المعلومات وأنظمة البيانات التي تعتمد عليها بشكل مباشر والتي ترتبط بالعمليات العسكرية . وتصنف حرب المعلومات إلى حرب المعلومات الشخصية: والتي تتضمن هجمات ضد خصوصية الأفراد وهجمات على الأجهزة الشخصية أو استخدام المعلومات الشخصية للأفراد، و حرب المعلومات الجماعية: وهي حرب يشترك فيها الشركات ويكون التركيز على المنافسة بين الشركات وسرقه الأسرار الاقتصادية، وحرب المعلومات العالمية: هذه الحرب يتم شنها ضد الصناعات ومستوى هذه الحرب يتم شنه من أكثر الأفراد مهارة من خلال الانترنت ونظم شبكة الكمبيوتر.

- الأمن الالكتروني:

ويعد الأمن security مفهوماً واسعاً يتعلق بأن الدول أصبحت في مأمن أو حماية من خطر التعرض للهجوم العسكري أو الإرهابي، وحماية أمن الكمبيوتر من المخترقين وحفظ الأمن من الآثار الضارة وغيرها، وفي هذه الحالة فان الأمن يصبح له بعدان بعد فني تكنولوجي والبعد الأخر يتعلق بالأمن بمفهومه الشامل الخاص بالدول، وتعني كلمة الأمن في مجال الفضاء الالكتروني بإجراءات الحماية ضد التعرض للإعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات، ومن جهة أخرى فان الأمن القومي يعني بحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، وتشير كلمة الأمن إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات.

و يشير الأمن عند توصيف الإجراءات الوقائية على الطرق العامة أو عند استعراض نظام حاسوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات. وقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لمفهوم الأمن. و لقد ظل هذا المجال من الأمن حتى أواخر السبعينيات معروفاً باسم أمن الاتصالات (Communication Security) (COMSEC) والذي حددته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي: "المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات" وتضمنت النشاطات المحددة لأمن الاتصالات COMSEC أربعة أجزاء هي: أمن التشفير Crypto security، أمن النقل Transmission Security، أمن الإشعاع Emission Security والأمن الفيزيائي Physical Security.

القوة المرنة:

يعد ذلك المفهوم قديم حيث استخدمه جوزيف ناي للتعبير عن الأدوات غير التقليدية أو العسكرية في تنفيذ السياسة الخارجية وحصرها في المساعدات الاقتصادية أو فرض العقوبات، فالقوة المرنة تساعد على تشكيل اتجاهات وسلوك الآخرين للقيام ما يريده من يمتلك تلك القوة استنادا إلى القيم والثقافة ولكن هذا المفهوم اتسع ليشمل، قوة المعلومات واستخدام الإعلام وتوظيفها داخل الفضاء الالكتروني ويشير أيضا إلى بعدين بعد يرتكز على حرب الأفكار وطرق الإقناع والتأثير والنفوذ والجانب الأخر يتعلق باستخدام الآليات الالكترونية كأسلحة الفضاء الالكتروني ومحاولة توظيفها عسكريا، وكذلك ما يتعلق باختلاف معايير القوة التي أصبحت تعتمد على قوة المعرفة والمعلومات والتي يكون لها تداعيات اقتصادية وسياسية في شكل مظاهر من مظاهر القوة، وأصبحت تكنولوجيا الاتصال والمعلومات لها دورا في نمو الاقتصاد العالمي فيما يعرف بالاقتصاد الرقمي.

## ثامنا: منهاجيه الدراسة

تحاول الدراسة الإجابة عن التساؤلات المثارة باستخدام ثلاثة مناهج هامة .

- منهج التحليل القانوني

حيث يتم تحليل مبدأ حظر استخدام القوة في العلاقات الدولية وكيفية تأثير الإرهاب الالكتروني وحرب المعلومات على ذلك المبدأ لكي يتم توضيح الفراغ القانوني والتشريعي في تناول تلك الظاهرة، وكيفية مواجهتها القانونية وطبيعة ونطاق الالتزام بحظر استخدام القوة في العلاقات الدولية وأثر ذلك

على مبدأ الأمن الجماعي، وعلاقة ذلك بالقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، وكذلك ما يتعلق بالمواءمة القانونية بين ما يفرضه الإرهاب الالكتروني من تحديات وما استقر عليه القانون الدولي من قواعد وأسس قانونية، وكيف يمكن الاستفادة من مبادئه العامة وأي من تلك الأطر القانونية الحالية يمكنها أن تتعامل معها وخاصة ما يتعلق بالقانون الدولي للبحار وكيفية إقراره مبدأ التراث المشترك للإنسانية وكذلك القانون الدولي للفضاء والأجرام السماوية والذي عمل على أهمية الاستخدام السلمي للفضاء الخارجي باعتباره ملكا للبشرية، وكذلك ما استقرت عليه قواعد العرف الدولي والاتفاقيات الدولية ذات الصلة في كيفية التعامل مع ما يطلق عليه بالمرفق الدولي.

- منهج تحليل النظام الدولي

يتعلق هذا المنهج بالإشارة لتأثير الثورة المعلوماتية على مرتكزات النظام الدولي وأصبح هناك مجتمع معلوماتي عالمي يشكل فيه وحدة التحليل الفضاء الالكتروني لما كان له من انعكاسات على انتشار مراكز القوة فيه مع عولمة الأمن والمنظمات الإرهابية والفاعلين من غير الدول وتأثير ذلك على مفهوم القوة والذي يعد من أهم أسس العلاقات الدولية، وكيف ساعدت في التأثير في آليات النظام الدولي في هيراركيته والتوازن داخله والتفاعل بين أطرافه، مع دور الثورة المعلوماتية في التأثير المباشر والتكاملي بين مناطق العالم وبشكل ظهر في زيادة تعقيد الظاهرة الدولية. وأثر التكنولوجيا في مدخلات ومخرجات النظام الدولي وزيادة مستوى التبعية التبادلية وكمية التفاعل بما أدى إلى تعقد مفهوم الأمن الدولي وتطوره من أمن الدولة إلى أمن المجتمع ثم أمن الفرد، وتعدد أطرافه الفاعلين من الدول وغير الدول وكثافة حركه التفاعل وأثرها في التداعيات الأمنية على النظام الدولي والاعتماد المتبادل بين وحداته وأثر ذلك على طبيعة القواعد المنظمة للعلاقات الدولية، وتحولت وحدة التحليل في النظام الدولي من السوق في المجتمع الصناعي إلى الفضاء الالكتروني في مجتمع المعلومات العالمي مع كون القوة التكنولوجية والعلمية أصبحت قوة قومية بعيدا عن المعيار العسكري المادي للقوة، وذلك لحساب تصاعد القوة اللينة في العلاقات الدولية وارتباط ذلك بتغير هيكل النظام الدولي بعد انهيار الحرب البادرة وبروز الولايات المتحدة كقطب أوحد، وما مثله من تحدي استخدام المتغيرات التكنولوجية والاتصالية لمزيد من الهيمنة والسيطرة على الدول الأخرى.

- المنهج الاتصالي:

حيث يتم اعتبار الفضاء الالكتروني منظومة اتصالية وهذا يعني أن جميع المواقع في الفضاء الالكتروني تهدف بشكل أو بآخر إلى إعلام المستخدم بشيء ما وبمكونات العملية الاتصالية، و يقصد بها ذلك المكون من العملية الاتصالية التي اهتم الباحث بالتركيز عليها من خلال دراسته للقائم بالاتصال و يقصد به كل الدراسات التي تتناول الانترنت والفضاء الالكتروني كمصدر للمواد الإعلامية، والاهتمام بالوسيلة: التي تعنى بدراسة الوسيلة نفسها وهي الفضاء الالكتروني، وهناك اهتمام آخر بدراسة الجمهور المتلقي للرسالة مثل مستخدمي الانترنت وحيث أن هناك شكلاً جديداً من الإعلام وهو الإعلام الإلكتروني ويتميز هذا النوع الجديد من الإعلام بسهولة إطلاقه في الإنترنت من أي مكان من العالم على خلاف وسائل الإعلام التقليدية المحدودة بمجال جغرافي معين. والدور الذي تلعبه في صياغة الخطاب

الإعلامي على مستوى العالم بما يعكس درجة التفاعل والجمهور الواسع عبر العالم وما شكله من وسيلة جاذبة لاستخدامها من جانب كافة الحركات الاجتماعية والسياسية للتعبير عن قيمها وأهدافها.

## تاسعا: تقسيم الدراسة:

للإجابة عن التساؤلات المثارة واستخدام المنهاجية سالفة الذكر تنقسم الدراسة إلى خمسة فصول تسبقها مقدمة وتنتهي بخاتمة حيث يتناول الفصل الأول: الأهمية الإستراتيجية للفضاء الالكتروني في النظام الدولي وينقسم إلى ثلاثة مباحث هي المبحث الأول يتناول الثورة التكنولوجية وظهور مجتمع المخاطر في النظام الدولي ويتكون من ثلاثة مطالب هي المطلب الأول: الثورة التكنولوجية والتهديدات الأمنية الجديدة ،والمطلب الثاني: بروز ظاهرة الفضاء الالكتروني في النظام الدولي، و المطلب الثالث: الفضاء الالكتروني و تغير طبيعة العلاقات الدولية ، والمبحث الثاني يتناول الطابع الالكتروني للأمن والقوة والصراع في النظام الدولي وينقسم إلى ثلاثة مطالب هي المطلب الأول: الفضاء الالكتروني وظهور القوة الالكترونية ، والمطلب الثاني: الأمن الالكتروني وإستراتيجية الأمن الدولي ،والمطلب الثالث: الفضاء الالكتروني والدبلوماسية" الالكترونية" وحل النزاعات الدولية ، وأما المبحث الثالث فيتناول أثر الفضاء الالكتروني على التفاعلات السياسية الدولية فيتكون من المطلب الأول: الفضاء الالكتروني والنظام السياسي الدولي، والمطلب الثاني: الفضاء الالكتروني والديمقراطية وحقوق الإنسان الرقمية ،والمطلب الثالث: أنماط التأثير السياسي للفضاء الالكتروني

ثم ينتقل الباحث إلى الفصل الثاني الذي يتناول فيه إشكاليات مفهوم الإرهاب الالكتروني والمفاهيم ذات الصلة والذي ينقسم بدورة إلى ثلاثة مباحث: يتناول المبحث الاول ماهية مفهوم الإرهاب الالكتروني وخصائصه، ويتكون من المطلب الأول: ماهية وإشكاليات مفهوم الإرهاب الالكتروني، والمطلب الثاني: خصائص الإرهاب الالكتروني ،والمطلب الثالث: آليات وأدوات الإرهاب الالكتروني والفاعلون .

والمبحث الثاني : هجمات الفضاء الالكتروني ما بين توصيف الإرهاب ومدلول الحرب ويتكون هذا المبحث من المطلب الأول: مفهوم الحرب ومجالها والأدوات والمسببات ،والمطلب الثاني: هجمات الفضاء الالكتروني ومفهوم الحرب غير المتماثلة ،والمطلب الثالث: هجمات الفضاء الالكتروني ومفهوم الإرهاب

، وأما المبحث الثالث فيتناول المفاهيم المرتبطة والمتداخلة مع الإرهاب الالكتروني، ويتكون من المطلب الأول: الإرهاب الالكتروني والجريمة الالكترونية، والمطلب الثاني: الإرهاب الالكتروني وحرب المعلومات ،والمطلب الثالث: المقاومة الالكترونية والاحتجاج الالكتروني وحرية الرأي والتعبير.

ويتناول الفصل الثالث تداعيات الإرهاب الالكتروني على الأمن والصراع الدوليين ينقسم لثلاثة مباحث الأول يتناول أبعاد وملامح تهديد الإرهاب الالكتروني لأمن المجتمع الدولي ويتكون من ثلاثة مطالب المطلب الأول: البنية التحتية الكونية للمعلومات وتغير طبيعة الأمن الدولي، المطلب الثاني: الفضاء الالكتروني كساحة للصراع والتنافس الدولي، المطلب الثالث هجمات الارهاب الالكتروني :حرب غير متماثلة وغير تقليدية ، أما المبحث الثاني فيتناول الإرهاب الالكتروني كشكل جديد من أشكال الصراع الدولي ويتكون من ثلاثة مطالب هي المطلب الاول : الفضاء الالكتروني وأجهزة الاستخبارات الدولية، المطلب الثاني: المطلب الثاني: استخدام الجماعات الإرهابية للفضاء الالكتروني، المطلب

الثالث :تنظيم القاعدة واستخدام الفضاء الالكتروني والمبحث الثالث: طبيعة وأنماط استخدام الفضاء الالكتروني في الصراع الدولي، ويتكون من المطلب الأول: استخدام أسلحة الفضاء الالكتروني في الصراع الدولي ،والمطلب الثاني: هجمات الإرهاب الالكتروني ونمط الحرب الباردة والصراع منخفض الشدة ،والمطلب الثالث: هجمات الإرهاب الالكتروني و نمط الحرب الساخنة والصراع مرتفع الشدة.

ثم ينتقل الباحث إلى الفصل الرابع الذي يعرض فيه موقف القانون الدولي من استخدام الإرهاب الالكتروني في الصراع الدولي وينقسم هذا الفصل إلى أربعه مباحث الأول يتعلق بطبيعة الجدل القانوني حول الموقف من هجمات الفضاء الالكتروني ويتكون من المطلب الأول :هجمات الفضاء الالكتروني والمبادئ العامة لمصادر القانون الدولي، ويتناول المطلب الثاني: هجمات الإرهاب الالكتروني كاستخدام للقوة في العلاقات الدولية والمطلب الثالث: الفجوة بين الأطر القانونية الدولية وهجمات الفضاء الالكتروني.، وأما المبحث الثاني: مدى إمكانية تطبيق القانون الدولي الإنساني على هجمات الإرهاب الالكتروني، ويتكون من المطلب الأول: مشروعية استخدام هجمات الإرهاب الالكتروني في حالة النزاع المسلح ،والمطلب الثاني: مشروعية استخدام هجمات الإرهاب الالكتروني في حالة الدفاع الشرعي،و المطلب الثالث دور محكمه العدل الدولية والمحكمة الجنائية الدولية ، والمبحث الثالث: الإرهاب الالكتروني وفق قانون الفضاء الخارجي وقانون البحار، ويتكون من المطلب الأول:التكييف القانوني للإرهاب الالكتروني في ظل قانون الفضاء الخارجي ،والمطلب الثاني: التكييف القانوني للإرهاب الالكتروني في ظل القانون الدولي للبحار . ويتناول المبحث الرابع الإرهاب الالكتروني وفق القانون الدولي لحقوق الإنسان ويتكون من المطلب الأول: الإرهاب الالكتروني وحقوق الإنسان الرقمية، والمطلب الثاني: الإرهاب الالكتروني والجدل ما بين الأمن والحرية. وأخيرا يأتي الفصل الخامس الذي يتناول: الجهود الدولية في تأمين الاستخدام السلمي للفضاء الالكتروني ويتكون من ثلاثة مباحث الأول يدور حول: الأمم المتحدة والاستخدام السلمي للفضاء الالكتروني فينقسم الى المطلب الأول: الأمم المتحدة وتنمية الوعي العالمي بالأمن الالكتروني، المطلب الثاني: القمة العالمية لمجتمع المعلومات وإدارة الانترنت،والمطلب الثالث: الاتحاد الدولي للاتصالات والمبادرة الخاصة بالأمن الالكتروني.ويتناول المبحث الثاني تطور الجهود والمبادرات الدولية للفاعلين داخل مجتمع المعلومات العالمي ويتكون من المطلب الأول: الجهود الدولية في مكافحة الإرهاب الالكتروني،ويتناول المطلب الثاني : المبادرات الدولية لتعزيز امن الفضاء الالكتروني ، والمبحث الثالث يتناول: نحو ميثاق دولي وثقافة عالمية لحماية الفضاء الالكتروني، ويتكون من المطلب الأول: الامن الالكتروني يدخل ضمن استراتيجية الامن الدولي ،والمطلب الثاني : الفضاء الالكتروني كمرفق دولي وتراث مشترك للإنسانية والمطلب الثالث يتناول نحو اتفاقية دولية للفضاء الالكتروني وتعزيز اطر القانون الدولي الحالي وتنتهي الرسالة بخاتمة تلخص أهم النتائج التي خلص إليها الباحث مع التوصيات التي تتعلق بتعزيز دور الفضاء الالكتروني في دعم السلم الدولي .

# الفصل الأول:

## الأهمية الإستراتيجية للفضاء الالكتروني في النظام الدولي

# الفصل الأول:
# الاهمية الاستراتيجية للفضاء الالكتروني في النظام الدولي

يحاول هذا الفصل ان يقدم لظاهرة الفضاء الالكتروني وتداعياتها الايجابية على المجتمع الدولي وكيف مثلت تظورا هاما من تطور المجتمع الدولي ، وفي نفس الوقت عكست تلك الظاهرة تزايد لدورها مع زيادة الاعتماد الدولي عليها في كافة الاصعدة السياسية والاقتصادية والامنية والثقافية وغيرها ، بشكل يعكس ظاهرة متعددة الابعاد تحوي مصالح الكترونية وفي نفس الوقت تتعرض لاخطار الكترونية ويتسع نطاق التحليل في الفصل الأول ليشمل- على الترتيب - المبحث الأول: الثورة التكنولوجية وظهور مجتمع المخاطر في النظام الدولي ، والمبحث الثاني : الطابع الالكتروني للأمن والقوة والصراع في النظام الدولي ، والمبحث الثالث: أثر الفضاء الالكتروني على التفاعلات السياسية الدولية

# المبحث الأول:
# مجتمع المعلومات العالمي
# وظهور مجتمع الخطر في النظام الدولي

**فرضت الثورة التكنولوجية مجموعه من التحديات والتهديدات الامنية الجديدة وبرز في النظام الدولي ما يعرف بالفضاء الالكتروني والذي اثر -بدورة - على التفاعلات السياسية والدولية الحاصلة بين مختلف الفاعلين في العلاقات الدولية المعاصرة، ويتم تناول ذلك وتوضيحة في هذا المبحث على النحو التالي : في المطلب الاول يتم تناول الثورة التكنولوجية والتهديدات الأمنية الجديدة ،والمطلب الثاني: بروز ظاهرة الفضاء الالكتروني في النظام الدولي ،و المطلب الثالث: الفضاء الالكتروني و تغير طبيعة العلاقات الدولية.**

## المطلب الأول:
## الثورة التكنولوجية والتهديدات الأمنية الجديدة

شهد العالم عدة تغييرات كان لها تأثيرها على طبيعة الأمن والصراع و بناء الدولة القومية في فترة ما بعد معاهدة ويستفاليا وحروب نابليون وبخاصة عندما تحولت المواجهة بين الجيوش إلى مواجهة بين الأمم، ما يُعرَف بتحويل الحرب إلى ظاهرة صناعية خلال الحرب العالمية الأولى واستخدام الأسلحة الذرية في نهاية الحرب العالمية الثانية، مما أسفر عن نتيجة مؤداها استحالة اندلاع الصراعات بسبب العواقب الوخيمة التي ستنجم عن تأثيراتها، واتسمت تلك الثورات في محيطها الأمني بخصائص مشتركة منها ما يتمثّل بفترة حضانة وببروز حدث مثير في معظم الحالات.

كما إن دوافع التغيير التي أحدثتها الثورة التكنولوجية التي تتكون في كل ثورة تقريباً من عناصر سياسية واجتماعية واقتصادية وتكنولوجية، بينما يمثل الجانب العسكري جزءاً محدوداً منها. وأصبح أحد الأوجه الأكثر تعقيداً في هذا الصدد يكمن في أن التغيير لا يشمل الجوانب كافة خلال المرحلة الثورية، إذ تشهد العديد من العناصر تغيرات كبيرة، بينما لا تتغير عناصر أخرى. وتكمن المخاطرة بالنسبة إلى أولئك الذين يواجهون العملية الثورية في كونهم يصبحون عاجزين حتى وقت متأخر عن تمييز العناصر التي تخضع للتغيير عن العناصر التي لا تتغير.

وأصبحت سرعة التغيير في العالم في أطره السياسية والاقتصادية والاجتماعية أصبحت تعبر عن دور ظاهرة العولمة بعد ما يقارب العقدين بعد انهيار الحرب الباردة في إحداث تغير أساسي في سمات الأخطار التي تهدد الأمن الدولي وما تعلق بارتفاع هامش عدم القدرة على التحكم في مهددات الاستقرار السياسي والاجتماعي والاقتصادي في كل من الدول المتقدمة والنامية، وذلك فيما يعرف بالأخطار الوظيفية والتي تضم المهددات متعدية الحدود التقليدية كأخطار التصحر وتغير المناخ والاحتباس الحراري وتلوث البيئة وثقب الأوزون وانتشار الأسلحة النووية والفجوة بين الشمال والجنوب والهجرة غير

الشرعية واللاجئين والجوع والفقر في العالم وغيرها.[1] وتحولت تلك الاخطار من مجرد تهديد للأمن القومي للدول إلى الأمن الإنساني الذي يتعلق بأمن الناس والبشر على الأرض.[2] وأصبحت القضايا ذات الطبيعة المحلية لها امتدادات عالمية كالحروب الأهلية والصراع العرقي والنظم الدكتاتورية في العالم النامي والتي أصبحت تمثل تحديا عالمياً جديداً مع انفتاح العالم على بعضه، وظهور الفاعلين من غير الدول (جماعات إرهابية، الحركات الانفصالية، الجريمة الدولية المنظمة، منظمات المجتمع المدني العالمي ) والذين أصبح لهم دور في التأثير على الأمن الدولي والخروج عن السيطرة التقليدية للدولة وزادت عملية تدويل القضايا المحلية واعتبارات التدخل الإنساني وحقوق الإنسان.[3]

وجاء ذلك الاهتمام العالمي مدفوعا بانهيار الحواجز بين الشرق والغرب وعولمة الاقتصاد والتطورات في المواصلات والاتصالات، وجاءت العولمة لتطرح تغييرات جدية على المصلحة القومية وعلى ماهية الحدود القومية والسيادة، وأصبحت المصلحة القومية غير مرتبطة فقط بحماية الحدود القومية والتي أصبحت أكثر اتساعا من خلال الانفتاح على الأسواق الدولية والاقتصاد وتعاظم دور المنظمات الدولية والشركات متعددة الجنسيات والفاعلين من غير الدول.

وأصبح الاعتماد على القوة العسكرية في تناقص لصالح الاقتصاد، وأصبحت مشكلة الأمن القومي تتعدى مجرد التدخل العسكري حيث أثرت العولمة على كافة عناصر القوة القومية والسيادة وأدت تلك التغيرات بدورها إلى اختلاف في درجات التهديد ومصادره وطبيعته وأثاره،

ولم يعد مفهوم الأمن القومي متعلقاً فقط بذلك الكيان المادي بل أصبح المفهوم الجديد يدور في فلك الحفاظ على سلامة الدولة في ظل تلك التطورات التكنولوجية ومن ثم اختلفت آليات التعامل. وأصبح الصراع انعكاساً للمرحلة التاريخية التي يمر بها وبيئة وسياق الصراع الدولي في ظل الموجة المعلوماتية التي يشهدها العالم ، وظهر ذلك في تغير طبيعة الصراع والقوة وممارستها وفي إحداث تغييرات داخل البيئة الأمنية للنظام الدولي.

واستخدمت تكنولوجيا الاتصال والمعلومات إما للتعبيرعن حالة الصراع وساحة له أو أنها تعمل في حل تلك الصراعات وتسويتها ،وأصبح الصراع يعنى بكل ما من شأنه التنافس والترابط التكنولوجي، وزادت الصراعات المرتبطة بهيكل وبنية المجتمع الدولي، وأرتبط شكل الصراع في عصر المعلومات بمعرفه من يعرف وأين ولماذا وكيف. وأخذت ظاهرة استخدام القوة في العلاقات الدولية شكلاً جديداً في طبيعة تلك القوة ووسائلها وأدواتها .

وشهد العالم بعد انهيار الاتحاد السوفيتي ظهوراً للقوميات والعرقيات على المستوى الدولي، وتفرد الولايات المتحدة بالنظام الدولي ومحاولة فرض قيم ونمط للعولمة على العالم في مواجهه ثقافات محلية

[1] Amitav Mallik," Technology and Security in the 21st Century A Demand-side Perspective", SIPRI Research Reports, hardback, Nov 2004,pp 23-164

[2] وقد دعت لجنة امن الإنسان بالأمم المتحدة إلى صياغة مفهوم جديد هو "الأمن الإنساني"، وقد صدر تقرير بنفس العنوان في نوفمبر ٢٠٠٤ تعبيرا عن التطور وطبيعة التحديات التي فرضتها العولمة والتهديدات غير التقليدية التي أصبحت تهدد الأرض وليس فقط دول معينة.

[3] د.مصطفي علوي "مفهوم الأمن في مرحلة مابعد الحرب الباردة "، في قضايا الأمن في أسيا "، تحرير (د.هدى متكيس، السيد صدقي عابدين )، مركز الدراسات الأسيوية، كلية الاقتصاد والعلوم السياسية، جامعه القاهرة، ٢٠٠٤.

تحاول الحفاظ على هويتها، وذلك في مقابل إمكانية التنميط والتماهي وسط ثقافة وافدة أعلى صوتا وأكثر انتشارا، وأدى ذلك لظهور جماعات وحركات راديكالية تحاول الحفاظ على قيمها إما بشكل سلمي أو في بشكل رد فعل عنيف في إطار عمل إرهابي أو حربي ضد ما تراه تهديدا لتلك القيم

ومع انتهاء الحرب الباردة وانتشار الموجة التكنولوجية التي اجتاحت العالم اتجه معها الصراع الدولي بالأساس نحو المغالبة والتنافس في ساحة الإنجازات الاقتصادية والنجاحات التجارية من فوز بتعاقدات وزيادة صادرات وانتزاع الفرص وصراع حول الأفكار والإبداع والذي أصبح يترجم في شكل منتجات تكسب أسواقا وتدر أموالاً، وسعت الأمم الظافرة بكل السبل للسطو على الأسرار الاقتصادية والتقنية والعلمية والتجارية للدول الأخرى وتغيرت أساليب الصراع الدولي مع ظهور تكنولوجيا الاتصال والمعلومات، وغلبة الصراع التقني والتجاري والاقتصادي على الصراع العسكري(١)

وأضاف الطابع التكنولوجي للصراع طرقاً بديلة عن الحرب المباشرة بين الدول أو بين الخصوم وظهرت تحديات جديدة تتطلب الاستجابة للأزمات الإنسانية والصراعات العرقية، وأصبحت تلك الصراعات تحتاج لتحالفات من الحكومة والمنظمات الدولية والقطاع الخاص، ومكنت الآليات التكنولوجية الحديثة على الجانب الاخر المنظمات من التنسيق بفاعلية بين جهودها، وإحداث التفاعل السياسي والاجتماعي والسياسي في إطار الآليات الالكترونية بعيدا عن الاتصال وجهاً لوجه، والعمل على تسهيل نشأة أشكال جديدة من التنظيم الاجتماعي وأنماط جديدة من الصراعات الاجتماعية – السياسية والصراعات الاثنيه والعرقية(٢)

وأصبح ذلك تعبيراً عن حدوث التغير الاجتماعي والسياسي الذي يصاحبه صراع خاصة على المدى البعيد، وفي حالة التغيرالسريع يأخذ الصراع أشكالاً سياسية واقتصادية واجتماعية ودينية وثقافية وبما وفر بيئة جديدة للعنف، فظهور نظام جديد يكون من شأنه إعادة توزيع الثروة والسلطة، والذي ما يلبث أن يواجه بمعارضة من المحافظين والراغبين في الإبقاء على الوضع القائم والقوانين التقليدية وشبكة العلاقات القائمة، وما يرتبط بها من الطابع الهراركي للسلطة والتوجهات الأخلاقية لنظام السابق.

وتصبح النخبة القديمة أمام خطر فقدان نفوذها وسيطرتها وقوتها، ومن ثم فإنها تحاول المحافظة قدر الإمكان على النظام الذي يشكل جزءًا من مصالحها، وفي المقابل يأتي مؤيدو النظام الجديد ليدافعوا عن مستقبله والراغبين في انتشاره وتظهر نخب جديدة لصيقة بهذا النظام الجديد، ويشكل ذلك دافعا للمقاومة من أجل التغيير، وهذه المقاومة قد تأخذ شكل المطالبة السلمية للتحرر، والتي تأتي في شكل ثقافي أو سياسي أو ديني ليمتد الصراع لما هو أبعد من الثروة والسلطة ليصبح صراع من أجل نمط حياة كاملاً وسياقاً حضارياً معيناً(٣)

(1) Steven Metz," **Armed Conflict In The 21st century:The Information Revolution And Post-Modern Warfare**", Strategic Studies Institute, U.S. Army War, April 2000 ,pp 5 -73
(2) Jerome C. Glenn and Theodore J. Gordon," **2004 State of the Future**", Chapter 5,Technology, The Millennium Project American Council for the UNU., Millennium Project Publications,2004 ,pp 1-401 .
(3) Alvin and Heidi Toffler " **Forword: the new intangibles** ", in Athena s camp: preparing for conflict in the information age ", Edited by John Arquilla & David Ronfeldt ", Santa Monica,CA:RAND,1997,pp 200-355.

ولعبت المعلومات دورا هاما في تاريخ الحروب سواء من خلال كيفية الحصول عليها أو استخدامها في تطوير أدوات القتال وعمل أجهزة الجيش، وبالمثل فقد ساعدت الثورة التكنولوجية في تغيير شكل الحرب وأدواتها وأثرت على الفاعلين بها، وساهمت في إعادة التفكير في حركية وديناميكية الصراع وأدى ذلك إلى اختلاف درجات التهديد ومصادرة وطبيعته وآثاره على المجتمع الدولي. ومن ثم فيمكن القول إن هناك شكلين من أشكال الصراع في عصر المعلومات هما حرب الشبكات وحرب الفضاء الإلكترونيCyber war & Net war ويشيران إلى النمط الخاص بطبيعة الصراع Cyber war, والتوجيه المعلوماتي الشامل للمعركة وتعد من الصراعات عالية الشدة high –intensity conflicts (hics) ، أما حرب الشبكات Net war فيمثل نوعا من الصراعات منخفضة الحدة Low-intetensity conflict (LIC) ، ،وعلى الرغم من زيادة معدلات استخدام تلك الأشكال إلا إن ذلك لا يعني بالضرورة اعتمادها فقط على الإنترنت أو وسائل تكنولوجيا الاتصال والمعلومات بل تأتي مواكبة أو معبرة عن استخدام الآليات التقليدية للصراع ولكن بوجه تكنولوجي يتواكب مع العصر.

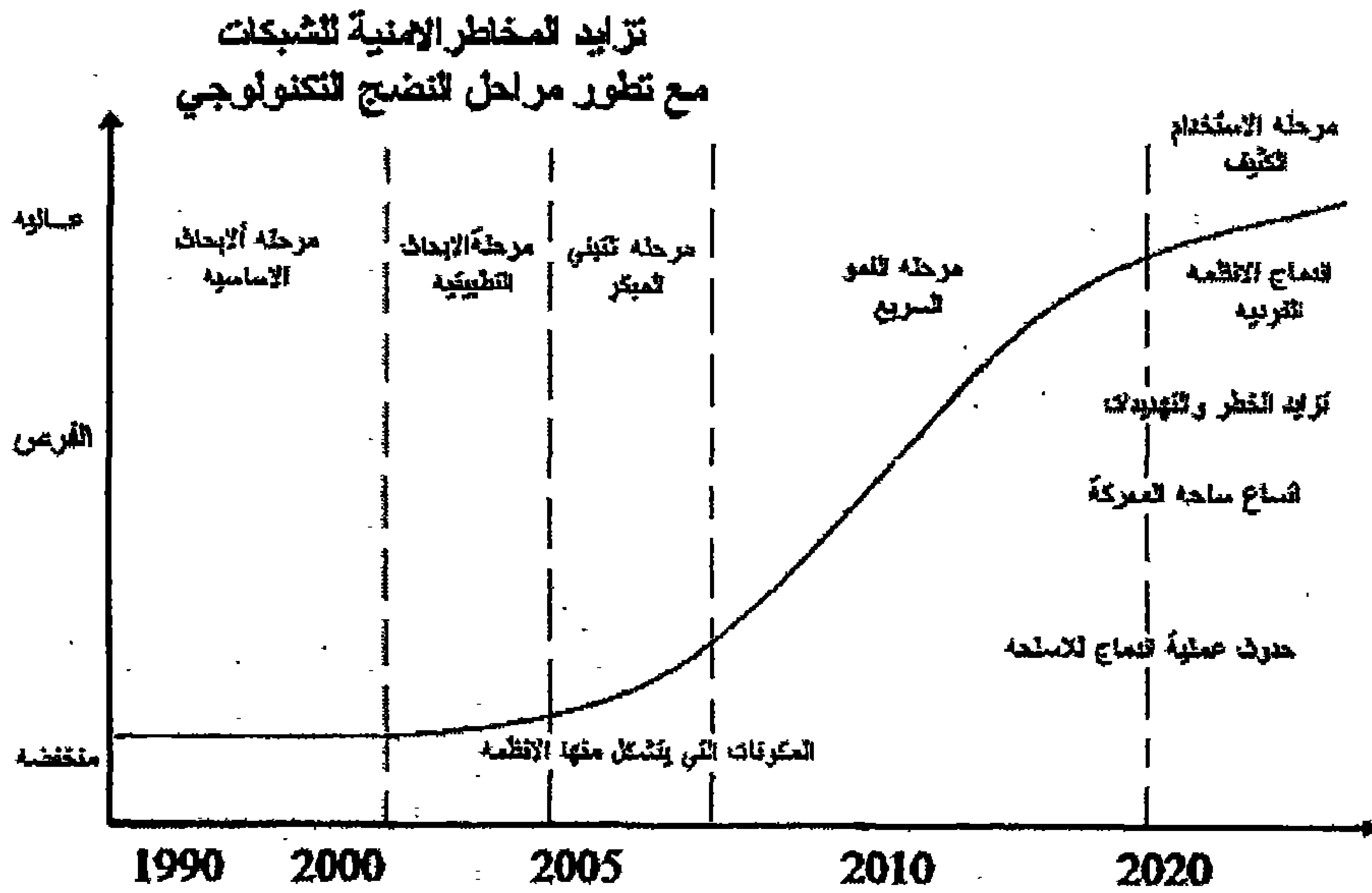
ويشير الشكل رقم (١) كيف إن المخاطر الأمنية تزايدت مع تطور مراحل النمو التكنولوجي في العالم، فكانت تلك المخاطر منخفضة في مرحلة الأبحاث الأساسية والتي تمتد في الفترة من ١٩٩٠-٢٠٠٠ ثم أخذت في الارتفاع البطيء في مرحلة الأبحاث التطبيقية في الفترة من ٢٠٠٠- ٢٠٠٥ وتلي ذلك زيادتها بشكل تدرجي متصاعد بدا من عام ٢٠٠٥ لتستمر في الصعود المتزايد في مرحلة النمو السريع في استخدام التكنولوجيا إلى إن تصل إلى مرحلة النمو الكثيف في الاستخدام حتى حلول عام ٢٠٢٠، وما بعدها.

ومن المتوقع أن تتميز مرحلة الاستخدام الكثيف للتكنولوجيا، وفي أواخر مرحلة النمو السريع بتزايد درجات الخطر والتهديدات واتساع ساحة المعركة وتنوع الوسائل مما يؤثر في حدوث عملية اندماج للأنظمة الفرعية وللأسلحة لتصبح أكثر ملائمة للتحديات الجديدة، وتصبح ثورة المعلومات عاملاً أساسياً في إحداث ثوره في الشئون العسكرية، وحدوث عملية الاندماج بين أدوات تكنولوجيا الاتصال والمعلومات على مستوى وظائفها، ومن ناحية أخرى دخولها لجميع مجالات وخدمات الحياة المدنية والبنية التحتية الكونية للمعلومات، وبما يكون له دوراً جديداً في صياغة الحياة الإنسانية.

وأحدث الانتشار المتصاعد لتكنولوجيا الاتصال والمعلومات انقساماً عالمياً عميقاً ومتزايداً بين الذين يملكون حظوظاً جيدة تتيح لهم إمكانية مضاعفة ثرواتهم من جهة، وأولئك الذين يجدون صعوبة في الارتباط بقيمهم الأساسية نظراً لانعدام الفرص التي تمكنهم من تكوين أي ثروات. كما يشهد العالم انتشار متزايد لتكنولوجيا الاتصال والمعلومات.

وأصبحت الدول تشهد تحدي لسيادتها من خلال اتجاه ايجابي في حدوث نزعة نحو تغيير البنية السيادية للدول، وما يتعلق بالحد من قوتها ونفوذها، من خلال الاتجاه نحو تجمعات أوسع وأكثر تمايزاً فوق المستوى القُطري. أما الاتجاه الثاني، وهو سلبي، فهو التحرك نحو إقامة الحكم الفاسد الذي يتسم بضعف قدرة الدولة إما على تدبير شؤون حياة مواطنيها ورفاهيتهم أو فشلها في إدارة علاقاتها مع دول أخرى مع جميع العواقب التي تترتب على ذلك، ويمكن أن يؤدي مثل هذا الوضع - في أسوأ الحالات

ـ إلى ظهور المنظمات الإجرامية التي تملك القدرة على زعزعة استقرار الأوضاع عن طريق استخدام العنف، مع ما ينجم عن ذلك من عواقب معروفة تشمل تفجر الصراعات العرقية- الاجتماعية- الدينية، وتفشي الإرهاب وانتشار أسلحة الدمار الشامل.[1]




*المصدر: Locationintelligence.net & Technolytics 2001-2004

شكل رقم (١)

و تميزت البيئة الإستراتيجية التي يعمل بها النظام الدولي بوجود عدد من مسببات الصراع مثل دور الجماعات الإرهابية والتنظيمات المسلحة التي تقف ضد الدول وترفض النظام الدولي القائم، وتعمل بكل ما أتيح لها من وسائل العنف والدمار على تقويض الأركان الأساسية لهذا النظام، بالإضافة إلى وجود الدول التي يحكمها قيادات راديكالية وتسعى للحصول على الأسلحة غير التقليدية، وهناك دول لا تستطيع السيطرة على وضعها الداخلي ودول فاشلة تمثل بداية بروز تنظيمات مسلحة وانتماءات أولية بها تسعي لتحقيق أهدافها بالقوة المسلحة، وهناك عنصر القوة المتزايدة لعدد لا بأس به من الدول، ويمكن أن تتفاعل كل تلك المكونات نحو زيادة عوامل عدم اليقين المولد لحالة الصراع.

وعلى قدر ما ساعدت العولمة في توليد الكثير من فرص التعاون والتقدم في مختلف أرجاء العالم فإنها عملت ايضا على خلق حالة من الانكشاف الأمني، و انتشارعوامل الخطر والاضطراب، مع زيادة حساسية الدول إزاء صدمات الأزمات العالمية. وأصبحت شبكة الإنترنت أحد معالم ذلك المجتمع وإحدى

[1] جيامباولو دي باولا ،" التحول في رؤيتنا للأمن" ،مجلة حلف الناتو ، العدد الثالث ، خريف ٢٠٠٦
(http://www.hq.nato.int/docu/review/2006/issue3/arabic/art2.html)

مؤسسات العولمة الهامة مع القوة الاتصالية العالية بين كافة إنحاء العالم ليصبح العالم كقرية صغيرة مع سرعة تدفق السلع ورؤوس الأموال والأفكار والبشر من مكان إلى أخر.

وعلى الرغم من التطور الهائل لثورة المعلومات وتكنولوجيا الاتصال عالميا، وما مثل ذلك من فوائد جمة للمجتمع البشري إلا أنها في ذات الوقت جعلت المجتمع الدولي يواجهه مخاطر جديدة مرتبطة بهذا التطور، وأصبح النمو المتصاعد لتكنولوجيا الاتصال والمعلومات واستخدامها في كل أوجهه النشاط الإنساني له دور في بناء مجتمع المعلومات العالمي، والذي يتميز بوجود اقتصاديات قائمة على إنتاج المعلومات وتوزيعها و مورداً استراتيجياً جديداً في نمو الاقتصاد الدولي، وذلك على حساب أهمية رأس المال والقوة العاملة و الموارد الطبيعه والمواد الخام ، و تحول اقتصاد الدول إلى جزء من اقتصاد عالمي متكامل ومتشابك يغلب عليه طابع التخصص والتكتل .

والى جانب ذلك ظهرت ثلاث طبقات من المخاطر البيئية والأزمات الاقتصادية الدولية والشبكات الإرهابية وتحمل تلك الأخطار علاقات ترابطية فيما بينها إلا أنها كذلك تحمل عدداً من الاختلافات على الأقل في طرق مواجهتها في ظل انهيار سيادة الدولة وتنامي الاعتماد الدولي المتبادل ، و تطورت أنماط الإرهاب في ظل بيئة دولية تميزت بعده خصائص لعل أهمها، اتساع نطاق العلاقات الدولية وسيطرة اقتصاد السوق واتساع الفجوة ما بين الشمال والجنوب، وضعف الطابع القومي للدول لصالح هويات مختلفة حتى داخل الدول ذاتها، وصعود دور الدين في العلاقات الدولية.، وظهوردور الثقافات المحلية مع تنوع المعتقدات والقيم الثقافية.

وجاءت الثورة التكنولوجية بمكاسب خاصة بفئات معينة دون غيرها وفقا للمستوى التعليمي والمادي، وأدى هذا التفاوت الى بروز احتقانات اجتماعية يتم التنفيس عنها من خلال استخدام العنف مع عدم وجود آلية سلمية للتعبير عن المصالح، وتواجه العديد من الدول تحديات تتعلق بشرعيتها مع انحسار دورها في المجال الاقتصادي، وصعود قوة الأسواق المالية والشركات متعددة الجنسية بالتزامن مع زيادة طابعها الدولي بما ساعد على الحد من قوة الحكومات الوطنية لصالح الجماعات تحت القومية، والتي تتفاعل مع بعضها دولياً دون العبور على الدولة الرسمية، وأصبح هناك حد من قوة الدولة وسيطرتها على تدفق رؤوس الأموال أو فرض العقوبات أو تنظيم عمليات الإنتاج وتعرضت سيادة الدول للتآكل.[1]

وأصبحت الجريمة العالمية عاملاً أساسياً في اقتصاد ومجتمع عصر المعلومات، وأصبحت العمليات الإجرامية أكثر تعقيدا وانتشرت الجماعات الإجرامية على نطاق عالمي مستفيدة بما وفرته العولمة من آليات وأدوات ظهر دورها في تحسين الاتصالات وتسهيل عملية انتقال الأفراد والأموال والأسلحة والأفكار، وبما كان لذلك من تداعيات على الأمن الدولي.

وتزايدت العلاقة ما بين التكنولوجيا والأمن لارتباط الدول بها في عمليات الاتصالات والإنتاج والخدمات، بما يجعلها في ذات الوقت تعتمد على أنظمة معلومات قد تكون هدفا سهلا للهجمات الإرهابية، ويأتي هذا مع محاولة الارهابين المستمرة في الحفاظ على تحديث أسلحتهم وإستراتيجيتهم،

[1] Todd A. Megill, **The Dark Fruit of Globalization: Hostile Use of the Internet.** Carlisle Barracks, PA, U.S. Army War College, 2005,.p.16.

وليصبح الإرهاب اكبر أحيانا من مجرد كونه إستراتيجية اتصال سياسي للقيام بهجمات بهدف التأثير إلى أقصى درجة في العامل النفسي لدى الجمهور أو الرأي العام، وكما تكون البنية التحتية الكونية للمعلومات هدفا ايضا لهجمات لتحقيق أهداف سياسية تخدم استراتيجية الإرهاب وليعكس ذلك تغيرا كبيرا في أنماطه ووسائله.

واتجهت وسائل الإعلام للانتشار بما يتلاءم مع تنوع المصالح على المستوى الدولي والمحلي ومستوى الفرد والجماعه، ويتم التعبيرعن تلك المصالح بالاستفادة من ثورة الإعلام والاتصال، وجذب ذلك الجماعات الارهابية، فقد استندت حركة الإرهاب الدولي خلال فترة الستينات على تأثيرها على ثورة الاتصال، والتي أوجدت لأول مرة في التاريخ نقلاً حياً للأحداث الإرهابية بما كان له تأثير واضح على الرأي العام الدولي.

وعلى الرغم من الاعتقاد بأن غياب القطبية الثنائية سيكون من شأنه الحد من ظاهرة الإرهاب الدولي حيث كان يستخدم كنمط من الصراع بين القوتين، كان هناك صعود للإرهاب الدولي ولكن بطابع أخر، وأصبحت المنظمات الإرهابية ليس لها علاقة بالدولة ولا تلقى بالضرورة دعمها بل أنها أصبحت تحمل إستراتيجية خاصة بها،

وهناك عوامل أخرى تتعلق بانتشار أسلحة الدمار الشامل واستمرار برامج الأسلحة البيولوجية والكيماوية، والتطبيق الواسع لتكنولوجيا الاتصال والمعلومات في المجالات الحيوية والمنشآت الاستراتيجية بما قد يحمل في مضمونه امكانية تعرضها لخطر الاستخدام الخاطئ أو التعرض لدرجات الأمان مع انتشار المعرفة التقنية والتعليمية الخاصة بالفيزياء أو الكيمياء أو البيولوجيا مع إتاحة المعلومات في ظل ظهور مجتمع المعرفة ، وذلك شأن خطروجود دول فاشلة يمكن أن يعرض قدراتها لخطر سيطرة جماعات إرهابية أو من دول اخرى معادية ، و دفع ضعف الدول في مجال شرعيتها ووظيفتها لقوة أطراف من غير الدول على المستوى المحلي مع إمكانية الحصول على الدعم الخارجي من أطراف أخرى، و زيادة دور المؤسسات الدولية والمجتمع المدني العالمي في العلاقات الدولية.(1)

وظهرت الحروب الجديدة في سياق دولي يغلب علية الطابع التكنولوجي، وذلك بخلاف الحروب القديمة بين الدول، والتي كان هدفها تحقيق اكبر درجة من الضرر للخصم والاستخدام المنظم للقوة في مواجهه قوة أخرى، ولكن نهاية الشكل القديم للحرب بين الدول لم يعن- بأي حال - انتهاء العنف، فشهد المجتمع الدولي بروز أنواع جديدة من العنف يمكن أن يطلق عليها "حروب جديدة "، وهذه الحروب يمكن أن تتم داخل الشبكات متعدية الحدود والتي قد تشمل دولاً وأطرافاً من غير الدول، ويكون هدفها ليس مجرد النصر العسكري بل قد يشمل التعبئة السياسية فقط بدلا من الإخضاع والسيطرة على إرادة الخصم، ويتم تعبئة المواطنين للمشاركة في المجهود الحربي سواء بالانضمام للجيش أو إنتاج أسلحة، وعلى عكس الحروب القديمة قد لا يتم توجيه العنف مباشرة

(1) Brynjar Lia," **The Impact of Globalization on Future Patterns of Terrorism**", Terrorism and Asymmetric Warfare Project, Norwegian Defence Research Establishment (FFI), PresentationOMS-Seminar 27 September 2000, Oslo-Norway

للعدو، و سهولة مد شبكات التطرف والعنف واختراق امن الدول الداخلي، ويكون هناك عدم اعتماد كامل على المعارك العسكرية التقليدية بل تاخذ صورا للتنافس والصراع على المعطيات التكنولوجية.

وظهرالارهاب الجديد كشكل جديد للتهديدات الأمنية الجديدة للمجتمع الدولي وأصبح أكثر إلحاحا من أنواع الإرهاب التقيلدي وذلك ينبع من خصائصه وآثاره وطبيعة أطرافة وإمكانية استخدامه في كافة الأنشطة الحساسة والأكثر تهديدا للأمن الدولي وظهر ذلك في تطور الإرهاب والجريمة الدولية.[1] وظهرت أشكال جديدة من الإرهاب هي:

١- الإرهاب التقليدي حيث شهد تطورا هائلا بفعل العولمة والتطور التكنولوجي بما جعل له بعداً كارثياً اكبر في الخسائر المادية والبشرية،

٢- الإرهاب النووي حيث المخاوف من حصول الجماعات الإرهابية على رؤوس نووية ووجود سوق سوداء لها بعد انهيار الاتحاد السوفيتي وعلاقة ذلك بجماعات الجريمة المنظمة الدولية،

٣- الإرهاب البيولوجي حيث شهد العالم بعض الحوادث حديثا كحوادث انتشار الجمرة الخبيثة وتتنوع الأسلحة البيولوجية إلى ثلاث فئات هي البكتيريا والجمرة الخبيثة والجمرة المتموجة والكوليرا والطاعون والفيروسات واشرها الجدري والتوكسينات، والسموم البكتيرية وأخطرها البوتيبولينوم والريسين ومن المحتمل إن تسعى الجماعات الإرهابية إلى استخدام تلك الأسلحة،

٤- الإرهاب الكيماوي ويتسم بالبساطة والسهولة النسبية بسبب سهولة تصنيع المواد الكيماوية وسهولة استخدامها علاوة على ضخامة الخسائر وينقسم إلى المواد الموجه ضد الأعصاب مثل السارين والخردل وفي اكس والثاني المواد الموجهة ضد الأنزيمات الموجودة داخل الجسم

٥ – الإرهاب الإلكتروني ويتمثل في استخدام شبكات المعلومات وأجهزة الكمبيوتر وشبكة الإنترنت من أجل التخويف والإرغام لتحقيق أهداف سياسية ويمثل الإرهاب الإلكتروني أحد مظاهر الانصهار بين العنف لأغراض سياسية وتوظيف التقنيات الحديثة في مجالات الاتصال والمعلوماتية، التي تعد إحدى أبرز آليات العولمة المعاصرة.

(1) Rohas Nagpal," **Cyber Terrorism In The Context Of Globalization**", II World Congress on Informatics and Law,Madrid,Spain,September 2002. (http://www.ieid.org/congreso/ponencias/Nagpal,%20Rohas.pdf)

## المطلب الثاني:
## بروز ظاهرة الفضاء الإلكتروني في النظام الدولي

هناك ثلاثة عناصر أساسية أفرزتها ثورة المعلومات هي المعلومات information و الفضاء الإلكتروني cyber و الطابع الالكتروني Digital، ويعد كلمة cyber مقتبسة من علم cybernetics وهو عبارة عن نظرية الاتصالات والتحكم المنظم في التغذية العكسية التي تعتمد عليها دراسات الاتصالات والتحكم في الحياة وفي الآليات التي صنعها الإنسان " وتعني التفكير المعقد في النظم الديناميكية عن طريق استخدام مفاهيم التحكم والتغذية العكسية، وظهر التطور العلمي في مسألة الدمج بين التكنولوجيا والجسم البشري، فيما يعرف بمصطلح "بيونيكس" bionics وهي مشتقة من الكلمتين biological&electronics وتعني بعملية الدمج بين المكونات الالكترونية بالمكونات البيولوجية للكائن الحي، ويدخل المصطلحان ضمن علم السيبرنيكا "cybernetics أي علم دراسة الاتصالات والتحكم الآلي في النظم العصبية للكائنات الحية ومحاكاة الآلات لها، وعدم النظم البيولوجية من خلال توصيلها بأعضاء صناعية أو نظم صناعية أخرى كما يهتم بفهم مبادئ التصميم البيولوجي والعمل على محاكاته.

وتمثل Cyber Theory، التي يشتق أسمها من الكلمة الإنجليزية المستعملة لوصف فضاء الإنترنت:"سايبرسبايس" Cyber Space.وترتكز إلى وجود الفضاء الافتراضي كحقيقة لها أبعادها المختلفة في الإنترنت... أما الكلمة نفسها"سايبر" التي صاغها الروائي ويليام جبسون، فقد وضعها حين بحث عن أسم ما لوصف رؤيته عن شبكة حاسوب كونيّة تربط الناس والآلات ومصادر المعلومات، والتي من خلالها يمكن المرء أن يتحرّك كأنه يبحر في فضاء افتراضي... وتُشتق الكلمة "سايبر" cyber من الفعل اليوناني "كيبرنو" kubernao الذي يعني"يقود" وتالياً تصبح "السبرانيّة" Cybernetics أسما لعلم الاتصالات والمعلومات والتحكّم. ولذا، تتلاصق تلك الكلمة أيضاً مع "الملاحة" navigation خلال فضاء من البيانات الإلكترونيّة، إضافة إلى التحكّم الذي يتحقّق عبر معالجة تلك البيانات."[1]

ويعد وليام جيبسون " William Gibson أول من استخدم كلمة cyber مقترنة بكلمة Space لتظهر في مصطلح الفضاء الإلكتروني " Cyberspace في كتابة الكلاسيكي عام 1984، وجاءت جهود "نيل استيفسون " Niel Stephenson عام ١٩٨٩ ليرسما معا صورة تكاد تكون شاملة عن ماهية ذلك المفهوم والتي تحددت في انه ذلك الفضاء أو المحتوى والبديل الكوني الذي يمكن من خلاله للناس أن تشارك فيه "[٢].

وتستخدم كلمة cyber مقترنة بكلمة space لتعبر عن أشهر تعبير في عصر المعلومات، واستخدمت cyberspace للتعبير عن الإنترنت في عام ١٩٩١، وأصبح هذا المفهوم أشمل وأوسع من الإنترنت ليضم

(1) علي محمد رحومة،"علم الاجتماع الآلي،"سلسلة عالم المعرفة،المجلس الوطني للثقافة والفنون والآداب،الكويت ٢٠٠٨،ص٤٥.
(2) Martin C. Libicki", Conquest in Cyberspace: National Security and Information Warfare",: Cambridge University Press; 1 edition (April 16 2007),the Rand cooperation 2007 ,pp 1-14

كل الاتصالات والشبكات وقواعد البيانات ومصادر المعلومات، وأصبحت بنية النظام الالكتروني تعني المكان الذي لا يعد جزءاً من العالم المادي أو الطبيعي حيث أنها ذو طبيعة افتراضية رقمية الكترونية تتحرك في بيئة الكترونية حيوية تعمل من خلال خطوط الهاتف وكابلات الاتصالات والألياف البصرية والموجات الكهرومغناطيسية. ووصف"وليام جيبسون " العالم الالكتروني بأنه "عبارة عن شبكات الكمبيوتر والاتصالات الالكترونية وعبارة عن شبكة كمبيوتر خيالية تحتوي على كم هائل من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة.

وتقترب العلاقة بين العالم المادي والعالم الواقعي بحيث يحصل مستخدمو الكمبيوترعلى خبرات لا وجود لها يكتسبونها عن طريق هذا الاستخدام فتؤثر بذلك المكونات الالكترونية على العالم المادي ".[1] والذي يمكن أن نسمعه ونراه ونحسه ونتأثر به ونقرؤه، وأصبحت قوة الكمبيوتر والشبكات تتزايد عاماً بعد عام لتجعل من السهولة إدراك وجود هذا المكون الالكتروني، وهذا ما جعل الناس يرون في الفضاء الإلكتروني على انه عالم موازي للواقع الذي نعيش فيه، ويعد الفضاء الإلكتروني عبارة عن فيض رقمي من المعلومات لا يعتمد كليا على البيئة المحسوبة التي توفرها شبكات المعلومات بل تتعامل أيضا بكثافة مع مفرداتة مثل سرعة تناقل البيانات وصلاحية الدخول إلى الشبكة بالإضافة إلى المعالجات التي تتناول البيانات المتدفقة ضمن البيئة الالكترونية "[2].

والفضاء الإلكتروني شأنه شأن ظاهرة الفضاء التقليدية التي تتألف من أربعه مكونات رئيسية هي المكان والمسافة والحجم والمسار ويعبر محتواها عن طبيعة وجود هذا المحتوى، ويتميز هذا الفضاء الإلكتروني بغياب الحدود الجغرافية وغياب الحكم القاهر لعنصر الزمن .[3] ويتطلب ذلك العالم الافتراضي لوجود هيكل مادي من أجهزة الكمبيوتر وخطوط الاتصالات، ومن ثم فان ما يعمل داخل هذه الأجهزة يمثل نمطا من القوة والسيطرة، حيث تصبح القيمة الحقيقية للفضاء الالكتروني هي القدرة على الاستفادة من كم المعلومات الموجودة داخله والمساهمة والتحكم بها في إطار وشكل الكتروني[4]،

والفضاء الإلكتروني عبارة عن مجال طبيعي ومادي ويرى آخرون انه ذا طابع افتراضي حيث يرونه بأنه " تلك البيئة الافتراضية التي تعمل بها المعلومات الالكترونية والتي تتصل عن طريق شبكات الكمبيوتر، كما يعرف بأنه"ذلك المجال الذي يتميز باستخدام الالكترونيات والمجال الكهرومغناطيسي لتخزين وتعديل أو تغيير البيانات عن طريق النظم المتصلة والمرتبطة بالبنية التحتية

(1) كما يحدد المجال البحري بجزئيات الماء (water molecules) وأساسيات قوة الموانع (principles of hydrodynamics)، كما يحدد المجال الجوي بجزئيات الهواء ومبادئ علم قوة الرياح (principles of aerodynamics)، كذلك يحدد مجال الفضاء الالكتروني بالمكونات الكهرومغناطيسية (electromagnetic spectrum) وبالالكترونيات المشاركة وبمدى انتشار الطاقة (Energy propagation)ويضم هذا كل الإشارات التي تنساب خلال المكونات الكهرومغناطيسية (EMS) من الهواتف المحمولة والانترنت وأجهزة الاتصال والمعلومات وهذه الإشارات إذا انبثقت أو انتقلت أو ارتدت فإنها تكون قد استخدمت الفضاء الالكتروني.

(2) Acicognani,"on the linguistic nature of cyber space and virtual communities", virtual reality ,vol.3,1998 ,pp16-24

(3) حسن مظفر الرزو،"الفضاء المعلوماتي"، مركز دراسات الوحدة العربية ،الطبعة الأولى، بيروت ٢٠٠٧ ،ص ص ٢١٣-٢٢٣

(4) Lt Col Paul D. Berg," Dominant Air, Space, and Cyberspace Operations," Air & Space Power Journal, Summer Issue – 2007.

الطبيعية "، ويعكس الخلاف حول طبيعة الفضاء الإلكتروني ما بين طبيعة افتراضية وأخرى مادية، ويحسم هذا الخلاف إن الفضاء الإلكتروني له طبيعة مادية وأخرى افتراضية تظهر في كونه مجالاً للحرب والقتال حيث تتحرك عمليات المعلومات التي تشير إلى البيئة التي يمكن من خلالها شن عمليات الهجوم والدفاع والتي تكون متصلة ومستخدمة عبرالشبكات ، بما يشير إلى إن كل مبادئ الحرب يمكن تطبيقها على الفضاء الإلكتروني مثل المجالات الأخرى [1].

ويشير الفضاء الإلكتروني كذلك إلى مجموعة المعلومات المتوفرة الكترونيا ويتم تبادلها وتشكيلها في مجموعات بناء على استخدامها، ويعمل الفضاء الإلكتروني تحت ظروف مادية غير تقليدية حيث يكون الفضاء الإلكتروني وسيطا عبر العمل من خلال أجهزة الكمبيوتر وشبكات الاتصال حيث يختلف عن الجو أو الفضاء الخارجي في أن الفضاء الإلكتروني يعمل وفق قوانين فيزيائية مختلفة عن قوانين الفضاء الخارجي، فمثلا لا تزن المعلومات شيئا ولا تمتلك كتلة مادية وبإمكان المعلومات أن تظهر للوجود وتختفي منه ويتم تعديل وتبادل المعلومات خلال نظم مرتبطة بالبنية التحتية.

ويتعامل الفضاء الإلكتروني مع المعلومات التي حيث تتوقف فائدتها إما من خلال تفاعلها مع غيرها من المعلومات أو إنتاج معلومات جديدة أو معلومات متوارثة تتفاعل داخل هذا الفضاء وخارجة وتشمل إما معلومات صحيحة أو مضللة، وليصبح التدفق الهائل للمعلومات داخل الفضاء الإلكتروني لا يقل عن قيمة هذه المعلومات،وترسم طرق الحصول علىهذه المعلومات شكل السلطة والقوة والتي تنقسم لمعلومات مجانية متوافرة لمن يريدها واخرى تجارية متوفرة لمن يرغب بالدفع ،وهناك المعلومات الإستراتيجية المتوفرة لمن يسمح له بمعرفتها فقط، وبإمكان هذه المعلومات داخل الفضاء الإلكتروني أن تتكرر بدون أي تكاليف وبالإمكان تجميعها دون تدخل من البشر وبالإمكان إن تنتقل من مكانها المادي، ولا يمكن إن تقتل ولكنها تقوم بذلك عندما تستخدم للتأثير من قبل لاعبين ماديين، ونظرا للطبيعة غير المادية للمعلومات فان وضعها في الفضاء الإلكتروني يجعلها متوافرة ومتاحة للجميع عالميا، وبذلك يعد الفضاء الإلكتروني وسيلة ورسالة حيث تتخذ المجتمعات شكلها وفقا لطبيعة الوسائل التي يتصل عن طريقها الأشخاص بدلا عن مضمون هذه الاتصالات .

والفضاء الإلكتروني غطاء ولكنة اكبر من الإنترنت لأنه يتضمن أيضا قدرات مثل توجيه الطاقة التي توجد في جزء من الموجات الكهرومغناطيسية، 'ويعد الفضاء الإلكتروني مكونا منشئا أي تم بناؤه من خلال الشبكات وأجهزة الكمبيوتر، وهو منتشر في أماكن متعددة في نفس التوقيت وذلك مشابه للفضاء الخارجي الذي يتكون من مجموعه من الكواكب والإجرام السماوية مختلفة الموقع ولكنها متعددة حيث يشمل الفضاء الخارجي كل ما هو فوق المجال الجوي للأرض، ولكن يختلف الفضاء الخارجي في انه يحكمه بعض الاتفاقيات الدولية كالتي تنظم الاتصالات أو البث الفضائي أو

[1] James M. Liepman, Jr.," **Cyberspace: The Third Domain**", Zel Technologies, LLC and Global Cyberspace Integration Center, November 15, 2007.
(http://www.au.af.mil/au/aunews/archive/0223/Articles/Cyberspace%20Third%20Domain%20-%20Liepman.pdf)

الإذاعي أو منع العمل على عسكرة الفضاء.[1] ويعد الفضاء الإلكتروني مجالاً عاماً وسوقا مفتوحة ويدلل على وجود شبكة من التواصل والعلاقات بين من يستخدمونه ويتفاعلون معه مع انتقال كافة مجالات الحياة من إعلام وصحة وتعليم وحكومة والمواطنة والاقتصاد والسياسية إلى الفضاء الإلكتروني فيما يشبه بالحياة الأخرى.إلى جانب ذلك أصبح الفضاء الإلكتروني وسيط ووسيلة في نفس الوقت لشن الهجوم وتنفيذ الإعمال العدائية بين الخصوم كغيرة من مجالات الجو أو الفضاء أو البحر، ليصبح وسيطا جديدا للصراع . ويحوي الفضاء الإلكتروني كماً هائلاً ومتسع عبر الشبكات ونظم المعلومات واتصاله وتداخله مع الفضاء الخارجي والأقمار الصناعية، وعلى الرغم من درجة التشابه بينة وبين الفضاء الخارجي إلا أنه يختلف في أن الفضاء الإلكتروني تم بنائه من قبل الإنسان ولم يوجد في الطبيعة، ويحكمه القانون الطبيعي مثل الفضاء الخارجي، كما إن الفضاء الإلكتروني تحكمه قوانين الوسط كأنظمة التشغيل والشبكات، بينما تنظم الفضاء الخارجي عدة اتفاقات دولية للاستخدام السلمي له [2]

وبينما تسيطر قلة من الدول على القدرات التكنولوجية لغزو الفضاء واستخدامه نجد أن الفضاء الإلكتروني على العكس حيث يمكن لأي دولة او فرد او جماعه أن تؤثر فيه وتتفاعل من خلاله مع الالتزام فقط بقواعد التشغيل ، وليكون بذلك ملعبا مفتوحا امام استخدام الجميع ، ويتكون الفضاء الإلكتروني من المكون الأول الطبيعي أو المادي والذي يتمثل في الأسلاك والمحولات والبنية التحتية المعلوماتية كالكابلات، والمكون الثاني يتمثل في المحتوى والذي يعكس شكل المعلومات في الفضاء الإلكتروني ،أما المكون الثالث فيتمثل في عملية التوصيل بين المعلومات والبشرويرتبط بتصورات الناس وثقافاتهم.

ولا يتكون الفضاء الإلكتروني فقط من شبكة من الاتصالات بل يتكون كذلك من المعلومات التي تنتقل من خلال هذه الشبكة أيضا واهم ما يميز مجتمع المعلومات هذا هو أن المعلومات المتوافرة لها قيمة اقتصادية وقيمة ميدانية بالنسبة إلى الجهات العسكرية وكلما زادت الفاعلية في إدارة تلك المعلومات كلما زادت الفائدة التي يمكن الحصول عليها وأصبح تفوق المعلومات إحدى القيم الأساسية للقوة العسكرية وأصبحت المعلومات مجالا للسيطرة والتحكم.

وأصبح للفضاء الالكتروني دور في التأثير على طبيعة الصراع و القوة التي تمارس من خلاله بالإضافة إلى طبيعة النتائج والآثار التي تنتج عنه، وهذا ما يعبر عن نوع جديد من ممارسة القوة عبر شكل جديد من أساليب الحرب الالكترونية عبر الفضاء الإلكتروني، وأثر ذلك على طبيعة القوة المسلحة ويأتي هذا مع خطر انتقال ساحة المواجهة في الحرب من الفضاء الواقعي إلى الفضاء الإلكتروني ليصبح هناك عالم آخر بديلا لما يدور على ارض الواقع، حيث يوجد مواقع انترنت ومتصلة بالأهداف الإستراتيجية والمرافق الحيوية يمكن ضربها، كما يمكن الدفاع والمقاومة لتظهر حرب

[1] Michael Wynne," Flying and Fighting in Cyberspace",Space Power Journal &Air, fall 2007 , pp1-11 also available at -last ( http://www.airpower.au.af.mil/apjinternational/apj-a/2007/fal07/wynne.pdf)

[2] يشير الفضاء الخارجي إلى المنطقة التي تلي مباشرة المجال الجوي للأرض ويتكون من مجموعه من الكواكب والأجرام السماوية.

جديدة بدون إراقة للدماء. ويمثل ذلك سلاحاً جديداً وفاعلين جدداً، فيما يشبه بحرب عصابات حيث تبادل هجمات الكر والفر ومن حروب الضربات الوقائية إلى حروب الوكالة والحروب السرية بشكل يبعدها عن مفهوم الحرب التقليدية المنظمة إلى نوع أخر من الحرب اقرب إلى مفهوم الإرهاب، وتمثل الإعمال العدائية التي تدور في الفضاء الإلكتروني وعمليات الدفاع والهجوم مشابها لمفاهيم القتال التقليدية إلا أنها تأتي في إطار الحرب الحديثة، كما إن الطابع الفردي لعمليات القتال تجعل هناك مجموعه متنوعة من الأعداء كما أن تحديد العدو وعملية السيطرة على الدخول تمثل تحديات لعمليات الفضاء الإلكتروني للقوات الجوية والتي يكون من مهامها التغلب والسيطرة عليها.(1)

وقد أقرت هيئة الأركان الأمريكية تعريفا للفضاء الالكتروني من وجهة نظر عسكرية بأنه" مجال يتميز باستخدام الالكترونيات والكهرومغناطيسية لتخزين تأثيرات متحركة أو ساكنة ضد الإشارات (الرادار- وأجهزة الاتصال) ونقاط ربط وشبكات النظام الدفاعي، حيث يتم الوصول إلى الهدف بسرعة الصوت أو بسرعة الضوء عند استعمال قدرتها الفضائية الالكترونية، و أعلنت القوات الجوية الأمريكية في ٧ ديسمبر ٢٠٠٥ تعريفا جديداً لمهامها القتالية "بان حددت مهمة القوات الحوية في تسلم المهام للدفاع عن الولايات المتحدة ومصالحها العالمية بقدرتها على الطيران والقتال في الجو والفضاء الخارجي وفي الفضاء الإلكتروني، "

وأصبح من مهام القوات الجوية منع هجوم الفضاء الإلكتروني للتعرض للبنية التحتية، والاستجابة السريعة للهجمات وإعادة الإصلاح للشبكات، والوعي الكلي بأهمية الفضاء الإلكتروني كساحة للصراع، والعمل على إلحاق الهزيمة بالخصوم والأعداء في ومن خلال الفضاء الإلكتروني بالإضافة إلى ضمان حرية الحركة للقوات داخل الفضاء الإلكتروني.

ومثل ذلك بداية إدخال الفضاء الإلكتروني ضمن القوات الجوية والتأكيد على دوره في القدرة العسكرية اللازمة للدفاع عن الدول ومصالحها، وتحول الفضاء الإلكتروني إلى مجال للعمليات العسكرية ومجالا لاستخدام القوة والسيطرة وذلك مع دوره في ظهور تحديات للعمليات العسكرية وتهديد للخدمات المدنية التي ترتبط بالبنية التحتية الكونية للمعلومات (2).

ودفعت عملية إدخال الفضاء الإلكتروني كمجال حربي لضرورة معرفة من هم الأعداء وكيفية محاولتهم للتدخل في الفضاء الإلكتروني وإفساد أو تعطيل عمل الخدمات المدنية أو العسكرية، وكذلك كيف يتم الاستخدام العسكري للموجات الكهرومغناطيسية التي تعتمد عليها القوات العسكرية اعتمادا كبيرا في عمليات القيادة والسيطرة، وهذا الاستخدام يتراوح من التعرض لهجمات منع وإنكار الخدمة أو التدخل في عمل الأسلحة الالكترونية وخاصة مع حرية الفضاء الإلكتروني التي تمكن الدول والفاعلين من غير الدول للاستخدام غير السلمي للفضاء الالكتروني، وخاصة مع انخفاض التكلفة والحاجة فقط إلى المعرفة والإمكانيات الفنية التي يمكن من خلالها دخول القوات

(1) Vincent Moscow, **The Digital Sublime: Myth, Power, and Cyberspace**. Cambridge, MA, MIT Press, 2004. 218 p.
(2)Patrick D. Allen, **Information Operations Planning**. Norwood, MA, Artech House, 2007. p323.

الجوية إلى الفضاء الإلكتروني، والذي أصبح مجالا أسهل من غيره من المجالات الأخرى حيث يتم شن الهجمات من أي مكان وفي أي وقت مقارنة بالحرب التقليدية وهذا ما يجعل هناك صعوبة أمام المقاتلين في الفضاء الإلكتروني لاكتشاف وتحديد مصدر الهجوم.[1] وأصبح الفضاء الإلكتروني لا يختلف عن المجالات الأخرى كالجو والبر والبحر فيما يتعلق بمبادئ الحرب وخصائص القوة حيث تسري في الفضاء الإلكتروني العقيدة العسكرية ذاتها والتي تركز على لامركزية التنفيذ ومركزية السيطرة، كما إن ذلك النوع الجديد من الحرب يأتي مشابها في أدواتها مع أدوات الحرب التقليدية من القذائف والصواريخ والدبابات والمتفجرات والحرب النفسية والتي تستخدم في ميدان المعركة إلا أن يتم استخدام أدوات أخرى شبيهه بها.

والتي تتميز عن غيرها من الأدوات التقليدية بانخفاض تكلفتها وطابعها الالكتروني الذي تتميز به وينعكس على قدرتها وتأثيرها المختلف واكلا محدود، مع تجاوز الفضاء الإلكتروني للحدود الدولية وتعلقه بعمل البنية التحتية الكونية للمعلومات، كما أن العمل العسكري أو العدائي يمكن إن ينتقل بسهولة من طابعه المحلي إلى إن يحدث تأثير عالمي ومنتشر عبر تمدد شبكات المعلومات والاتصال في زمن قياسي لا يتعدى المللي من الثانية.

وأصبح الفضاء الإلكتروني يحوي أيضا شبكات اجتماعية وتواصلاً على المستوى الدولي عبر ما يزيد على ١، ٨ بليون مستخدم ينتشرون في ٢٢٥ دولة وما يزيد على مليار مستخدم للانترنت عالميا ووجود مجتمعات افتراضية تجمعهم ميول مشتركة ومتشابهة مثل موقع faceook وموقع Xanga وموقع My space وموقع Hi5 ومثل ذلك ظهور نوع جديد من التفاعلات الدولية وأصبح الفضاء الإلكتروني وسيلة إعلام ودعاية دولية ومنبرا للرأي العام الدولي بشكل قامت تلك المواقع في دورها مقام المنظمات الدولية والحكومية في مناقشتها للقضايا الدولية.

## المطلب الثالث:

## أثر الفضاء الالكتروني على تغير طبيعة العلاقات الدولية:

كان هناك عدد من العوامل ساهمت في بروز شكل جديد من استخدام القوة في العلاقات الدولية بعد أحداث ١١ سبتمبر ٢٠٠١، وظهر بشكل اوضح تغير في طبيعة الهيمنة والنفوذ، والتي كانت تستند للقدرات العسكرية وحدها لتعتمد بصورة أكبر على القدرات الاقتصادية والتكنولوجية، و تراجع في أهمية القضايا الخاصة بالصراع الأيدلوجي بين الشرق والغرب وخاصة بعد انهيار الحرب الباردة لتحل محلها قضايا عالمية تتعلق بالأمن الإنساني المشترك، وتصاعد دور الدين في العلاقات الدولية في إطار تحول العالم من الاهتمام بالقيم المادية إلى ما بعد المادية، والتحول من

[1] James M. Liepman, Jr, Op.Cit. pp 12-15.

الشمولية إلى الديمقراطية وانفتاح العالم على بعضه البعض ليصبح قرية صغيرة مع دخول تكنولوجيا الاتصال والمعلومات كافة المجالات المدنية والعسكرية.

وأدت تحولات ما بعد الحرب الباردة لوجود أنماط جديدة من العلاقات الاجتماعية والرؤى السياسية، وبرزت على الساحة الدولية هويات وانتماءات مختلفة وأكثر تنوعا مع ضعف الدولة القومية، كما حدث إضفاء لمزيد من القوة على جماعات وأطراف من غير الدول كمنظمات المجتمع المدني والشركات متعددة الجنسيات، وأصبح هناك قيود على قدرة الدولة على صنع السياسية الخارجية بل لم تعد الفاعل الاوحد في العلاقات الدولية ، وتاثير ذلك على وظائف الدولة وهياكلها وعلاقة القوة سواء داخلها او مع غيرها في المجتمع الدولي ، وتغيرت أسس الشرعية التي كانت تستند إليها ، وليدفع ذلك العالم ليصبح وحدة واحدة من وحدات التحليل في علم السياسة بدلا من الدولة أو القبيلة أو المجتمع المدني.

و برزت فكرتان أساسيتان هما التميط والهيمنة وبث رؤى عالمية أحادية و القدرة على تنوع المجتمع الدولي في إطار اختلافاته الثقافية والعرقية [1] ،واخذ ذلك المزيد من الزخم الدولي بعد انتهاج الولايات المتحدة الضربات الوقائية في إطارما تدعية من الحرب على الإرهاب على تنظيم القاعدة ، وشكل ذلك النهج تهديداً للنظام القانوني الدولي و فاعلية المنظمات الدولية كالأمم المتحدة. وبرزت أطراف أخرى فاعلين في الصراع الدولي بما أثرعلى إضعاف شرعية الدول وسيادتها الإقليمية .

وأصبح هناك ترابط متزايد بين الدول وبعضها البعض و ما بين داخلها والخارج. وأثرت الثورة المعلوماتية على إعادة توزيع وتغيير الأوزان النسبية للفاعلين في النظام الدولي، وذلك ليس فقط وفق الموازين التقليدية كالقوة العسكرية بل أصبحت تميل لصالح القوة العلمية والتكنولوجية [2]، وشهد النظام الدولي قدرا من التعاون بين وحداته إلى جانب قدر من الصراع، وأصبح من الصعب تحديد مفهوم واضح للعدوان باعتباره عملاُ عسكرياً غير مبرر تقوم به الدولة ضد دولة أخرى مع ظهور الاعمال العدائية عبر وسيط ومجال جديد هو الفضاء الالكتروني وما انطوى على ظهور استخدام جديد للقوة والعدوان ، وكان لذلك تأثيرعلى فاعلية النظام القانوني الدولي باعتباره الأداة الحاكمة المنظمة لحركة التفاعلات داخل النظام الدولي، والذي بدا عاجزاً عن مواكبة التغييرات التكنولوجية وبما يمكنة من التعامل مع ظاهرة العدوان واستخدام القوة بشكل غير تقليدي لا يقتصرعلى استخدام القوة العسكرية التقليدية، بعد أن أصبح الفضاء الإلكتروني وسيطا في علاقات الدول ببعضها على المستويات السياسية والاقتصادية والاجتماعية والعسكرية والاعلامية، وتاثيرأعلى النظام الدولي وعلى التوزيع العالمي للقوة والثروة وعلى سيادة الدول، والتوجه نحو الديمقراطية ،و ما مثلة ذلك من تحديات تفرض على الفاعلين التكيف معها.

(1) د.علي الدين هلال "اثر العولمة على علم السياسية "، د.حسن نافعة &د.سيف الدين عبد الفتاح (محرران) ، سلسلة محاضرات الموسم الثقافي (١) قسم العلوم السياسية ،جامعه القاهرة ،٢٠٠٠.

(2) Eugene B. Skolnikoff," **Will Science and Technology Undermine the International Political System**", the 2001 Loewy Memorial Lecture given at the Edmund A. Walsh School of Foreign Service, Georgetown University, Washington, DC, March 13, 2001.

واصبح يشهد المجتمع الدولي صورة متزايدة من الاحتكاك والتفاعل في حياتهم اليومية مع ثقافات مختلفة ويتعرفون على إنسانية متعددة الأوجه، وظهرت صعوبة في السيطرة التامة على نوع وكم المعلومات والتي تصل إلى عقول الأشخاص بما يكشف عن حدوث تفاعل حضاري بين ثقافات متنوعة، و يعكس في الوقت نفسة خطورة رد الفعل العكس السلبي تجاه ذلك التفاعل او استخدام تلك الحرية على نحو يضر بمصالح الجماعه الدولية من قبل قوى وجماعات تحمل أجندة سياسية مختلفة.

وأصبحت الأنشطة المدنية والعسكرية تعتمد بشكل كثيف على تكنولوجيا الاتصال والمعلومات ومجموعة متنوعة من نظم المعلومات الرئيسية و أكثر ارتباطا فيما بينها، وأصبحت تدخل في البنية التحتية الحيوية وتمثل ركيزة لقيامها بخدماتها وفي النمو الاقتصادي وفي الجيش والدفاع والاتصالات والتجارة وكافة مجالات الحياة.[1] وأصبحت شبكات الاتصالات ونظم المعلومات عاملا أساسيا في التنمية الاقتصادية والاجتماعية ودخلت الحوسبة والتشبيك في كل المرافق الحيوية كالكهرباء وإمدادات الميناء والسدود وخزانات الطاقة والمطارات والإدارة الالكترونية ونقل المعلومات والدفاع والبنوك والتجارة والمواصلات وعقد الصفقات والبورصات العالمية[2].

وحمل ذلك في طياته إمكانية التعرض للأخطار التي قد تهدد بالهجوم على الأهداف الاستراتيجيه القومية حيث بإمكان الفاعلين من الخارج أو الداخل في مجتمع المعلومات العالمي، حيث يمكنهم القيام باعتداءات عن طريق استخدام أسلحة الفضاء الالكتروني بهدف إلحاق بالغ الضرر بالبرمجيات المشغلة أو ما يتعلق بالمعدات والبنية التحتية ونظم التحكم والإشراف على العمليات الإنتاجية فيما يعرف بنظام "سكادا " SCADA، وارتباطة بعمليات إنتاج وتوزيع الكهرباء والمواصلات والخدمات المالية والاتصالات وإمدادات المياه، وأصبحت تلك الأخطار لا يمثل مصدرها فقط الدول بل من فاعلين من غير الدول.[3] ودفع ارتباط تلك الخدمات بالفضاء الالكتروني الى ان اصبحت سيطرة الدولة على امنة ضعيفة ومن السهولة التاثير علية عبرآليات سهلة ومتنوعه بما يعمل على التأثيرعلى عملها واختراقها او تدميرها، وياتي هذا مع زيادة حجم الفاعلين مع زيادة قابلية المرافق الحيوية المدنية والعسكرية للخطر، وظهر تلك الاخطار ضمن غيرها من الاخطار متعدية الحدود وغيرالتقليدية، وليدخل الارهاب الالكتروني ضمن غيره من الاخطار ذات البعد الدولي كالانتشار النووي والجريمة الدولية وتجارة المخدرات والكوارث البيئية وانتشار الأمراض المعدية، وغيرها من قضايا تدخل في اطار التداعيات الامنية للعولمة.[4] وساهم الفضاء الالكتروني في اضفاء المزيد من القوة على المجتمعات المحلية والفاعلين من غير الدول، وعلى الجانب الاخر عملت على المساهمة في تهميش بعض الجماعات والتي حملت رؤية

---

(1) امل محمد فوزي منتصر"، "مجالات استخدام شبكات المعلومات الدولية "الانترنت"في الأنشطة الاتصالية "رسالة ماجستير غير منشورة، جامعه القاهرة، كلية الإعلام، ٢٠٠٤ ،ص ص ٢٠٠-٢١٣.

(2) Kasia Wichrowska, **Advancements in Information and Technology and International** Security, North American Model United Nation 2006. ( www.namun.org/dp/DISEC2.pd)

(3) Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson," **Strategic Information Warfare: A New Face of War"**, National Defense Research Institute, RAND Corporation, 1995, pp125.

(4) Lynn E.Davis, **"globalization's security implications"** .Issue paper ,RAND,2003.

سلبية للتقدم التكنولوجي في انه أداة لسيطرة من يملك على من لا يملك وبرزت تحديات تتعلق بالتكامل السياسي والعرقي داخل الدول، وأدي ظهور شبكات تكنولوجيا الاتصال والمعلومات لانتقال القوه لفاعلين ليسوا بدول والذين يمكنهم إن ينظموا أنفسهم في شبكات تنظيمية متعددة تتسم باللامركزية، وتكون أكثر مرونة واستجابة لأي رد فعل تجاه التطورات الخارجية، وتحسين قدرة هؤلاء الفاعلون على تحسين عملية صنع القرار بداخلها، وظهرت الصراعات التي تعتمد على قضايا المعلومات والاتصالات ويدور حول المعرفة والاستحواذ على القوة الناعمة، وأثر ذلك في إحداث تغييرات كبرى فيما يتعلق بتحديد طبيعة الخصوم وشكل التهديدات وما يزيد من الطابع النفسي للخطر، ووجود قدر من الغموض حول تلك الأخطارمتعددة الأبعاد والقابلة للانتشار.[(1)]

وساهم النمو في مجتمع المعلومات في زيادة معضلة الأمن حول ضمان سرية البيانات وإرسالها واستقبالها وتخزينها ومدى تغييرها وتأمين الثقة فيها وحماية نظمها من الهجمات، خاصة مع بروز أخطار إرهابية وإجرامية او اداة في يد الدول لمارسة اعمال عدائية تجاه بعضها البعض، وذلك مع الاعتماد القوى على تكنولوجيا الاتصال والمعلومات في النظم المالية والاقتصادية والسياسية وفي تقديم الخدمات الحكومية، واعتماد النشاط الاتصالي وارتباطه بالبرامج الالكترونية الخاصة بالعمليات العسكرية و تطور وعمل الأسلحة [(2)]. وياتي هذا مع توسع عدد مستخدمي الفضاء الإلكتروني عالميا، من مليار إلى ٤ مليارات نسمة بعد انضمام شريحة مستخدمي التليفون المحمول وهم حوالي ٣ مليارات نتيجة خدمات الأجيال المتطورة، والتي تجعل لمستخدمي المحمول ip خاصا بهم، وظهور تلاحم بين خدمات الاتصال والإعلام والمدني والعسكري.[(٣)]

وطرح هذا التقدم المدني السلمي للثورة التكنولوجية إمكانية استخدام تلك المقدرات على نحو عسكري عدائي على نحو يشبه مختبرات مراكز الإبادة، ومن ثم فإن تكاثر فرص امتلاك الدول للمقدرات النووية والكيماوية والبيولوجية جعل هناك تسارعا محموما من أجل السبق في امتلاك أحدث تقنياتها وأدواتها في ظل سوق عالمي مفتوح، وبالمثل ظهرت محاولة الاستحواذ على القوة الالكترونية داخل الفضاء الالكتروني كجزء من المنافسة من أجل فرض الهيمنة بدلا من الأسلحة التقليدية في الفضاء الواقعي، واستخدام اسلحة الفضاء الإلكتروني كنظام تسليحي جديد، مع أهمية للبنية التحتية الكونية للمعلومات، وبما يعرض الدول لخطر التحكم في تدفق المعلومات ونقلها وتشكيلها وطريقة بثها مما يؤثرعلى الاقتصاد والأمن الدوليين.

ولا تعتمد القوة في عصر المعلومات كثيرا على الأرض أو القوة العسكرية أو الموارد الطبيعية فقط بل تعتمد اكثر على المعلومات والتكنولوجيا، وظهر ما يعرف بالقوة المرنة كالمعرفة والمعلومات

[(1)] **Diversification Of Cyber Threats**, Trustees of Dartmouth College (Institute for Security Technology Studies). U.S.Department of Justice. MAY 2002 (http://www.ists.dartmouth.edu/analysis/dct0502.pdf)

[(2)] CPT Ow Kim Meng, **Cyber-Terrorism: An Emerging Security Threat Of The New Millennium**, POINTER, the official journal of the Singapore Armed Forces, V28 N3, Jul - Sep 2002. (http://www.mindef.gov.sg/safti/pointer/back/journals/2002/Vol28_3/6.htm)

[(3)] وياتي هذا مع اندماج الوظائف ما بين الانترنت والهاتف المحمول والتلفزيون والراديو والتطور الهائل في الوسائط المتعددة والتي تمثل مايطلق علية الفضاء الالكتروني حيث تعتمد على الموجات الكهرومغناطيسية .

والمعتقدات والأفكارعلى الصعيد الدولي، والتي اصبح دورها في التصاعد عالميا مقابل الأخرى الصلبة والتي يتم استخدامها من قبل الفاعلين في مجتمع المعلومات العالمي لتحقيق أهدافهم. وأصبح هناك اهتمام متزايد لاستخدام مجال المعلومات والفضاء الإلكتروني كمجال استراتيجي مركزي في حالة شن حرب عبر شبكات المعلومات، وأصبح اللاعبون الصغار يمكنهم أن يدخلوا في الصراع بناء على استخدام استراتيجيات غير متماثلة تلائم قدراتهم وتعطيهم قوة نسبية كبيرة، وكما تجعلهم على قدم المساواة في الفرص مع القوى الكبرى ولديهم قدرة هائلة من المرونة والسرعة والحصول على المعلومات.

وزادت أهمية القوة المرنة بالاعتماد على طرق الإقناع والتأثير في الرأي العام العالمي، والقدرة على التعبئة والحشد والحصول على المساندة، وأدى ذلك لوجود زخم كبير من حجم الفاعلين في العلاقات الدولية والتأثير على عملية صنع السياسة الخارجية للدول والسياسة الدولية بصفة عامه، واصبح لتلك القوة الجديدة تأثيرات على كافة المجالات وأنماط الحياة على مستوى العالم، ولها دور في التأثير في المجال السياسي عن طريق تدفق المعلومات، وكذلك التأثير في المجال الاقتصادي حيث تتحول المعرفة إلى قوة أساسية أقوى من قوى الإنتاج. وبذلك تحول الأقتصاد الدولي إلى اقتصاد خدمي يعتمد على المعرفة وانتاج المعلومات والابتكار بخلاف الاقتصاد القديم الذي كان يتميز بالاعتماد على السوق التقليدي والكثافة العمالية والإنتاج الوفير، وكانت فية القوة الاقتصادية ترتبط بالقدرة على امتلاك المواد الخام والموارد الطبيعية، ولكن ما يعرف بالاقتصاد الرقمي الجديد اصبح يرتبط بالتطور التكنولوجي والمعلوماتي وظهور مؤسسات عمل غير تقليدية ونظم ادارة الكترونية ومنتجات تعتمد على الابتكار والسرعه و تضاؤل قيمه المكون المادي وارتفاع قيمه المكون المعلوماتي.

وأثر الفضاء الالكتروني على المجال الاجتماعي الدولي في زيادة المعلومات التي يكون لها دوراً في ظهور أنماط تغير القيم السائدة وعلاقات العمل وهيكل القوة داخل المجتمع، والتأثير في المجال الإعلامي مع زيادة مؤسسات الإعلام والفاعلين فيه ، وقدرته على الكشف عن قضايا المجتمع الدولي بصورة متنوعة وسريعه ، وإجراء التبادل الذي يعتمد على المشاركة بين ( المرسل+المستقبل) بأساليب متطورة دون وسائط بشرية، وكان من شأن كل تلك المظاهر أن كان لها دور بصفة عامه في تغير طبيعة المكونات والفاعلين وأجنده ونمط الاتصال والاستجابة داخل النظام الدولي .[1]

وأصبح الفضاء الالكتروني قاطرة التقدم في العصر الالكتروني، وعمل على تمكين المواطنين داخل المجتمع الدولي من الدخول بوسائل متعددة، وجعلت هناك أفكاراً وتغيراً في طرق ونمط الحياة ، ولا يحتاج الأمر سوى وجود جهاز كمبيوتر ونقطة اتصال بالإنترنت، كما عمل ذلك على دعم الجهود لفهم العالم بصورة أفضل وانفتاح أجزائه على بعضها البعض بما جعل هناك دعماً للرأي العام الدولي ،والذي يمثل بدورة ضغطا على الحكومات الرسمية في العالم ،و زيادة حجم التفاعل الرسمي وغير الرسمي بين وحدات النظام الدولي وكان لذلك تأثير على سيادة الدول بعد أن كانت الأسس والأطر

[1] Alan J.Rosenblatt," **International Relations in Cyberspace**", presentation at the 40th annual meeting of the International Studies Association, Washington, D.C., February 16–20, 1999 (http://www.ciaonet.org/isa/roa01/)

النظرية التي قامت عليها العلاقات الدولية منذ اتفاقية ويستفاليا عام ١٦٤٨ قائمة على مسألة الفصل ما بين العلاقات الداخلية للدولة والخارجية لها، و ترسيخ مبدأ سيادة الدول وعدم التدخل في شئونها الداخلية واحترام استقلالها. ولكن جاءت الثورة التكنولوجية في العالم لتؤثر بشكل تدريجي ومتصاعد على النظرة التقليدية للأمن والقوة في العلاقات الدولية إلى الدرجة التي أصبح فيها من الصعب الفصل بين ما يعد شأنا داخليا وأخر خارجيا، وظهر فاعلون من غير الدول وقوى جاءت مستفيدة من العولمة التي أصبحت سمة المجتمع الدولي الحديث.

واستخدم الفضاء الإلكتروني في شحذ الاهتمام بقضايا دولية مثل الإرهاب أو الفقر أو المرض أو الاحتباس الحراري وغيرها من القضايا ذات الطابع الإنساني. وساهم في زيادة حركة التفاعل في كافة جوانب المجتمع الدولي الاقتصادية والسياسية والثقافية والاجتماعية، واستخدم كذلك الفضاء الالكتروني كوسيلة إعلام دولية يتم توظيفها لشن حملات إعلامية ذات أهداف خاصة وعامة سواء في حالة الحرب أو السلم، ويتم من خلالها الكشف عن التجاوزات أو القضايا أو الكوارث الطبيعية، ولكي يتم تفاعل الرأي العام العالمي حولها، وأصبح الفاعلون المحليون لهم دور في السياسة الدولية وفي حركة التفاعل بين الدول.

وهذا ما أدى لوجود شبكة معقدة من العلاقات داخل النظام الدولي يتداخل فيها ما هو محلي بما هو دولي، وأصبح التحدي السياسي الهام هو كيفية الموازنة ما بين دور القوى المحلية والدولية في صنع السياسة العالمية، وأصبحت درجة التشبيك العالية لشبكات المعلومات تتخطى السيادة الإقليمية للدولة على أراضيها لصالح تقديم خدمات عالمية كمرور كابلات الاتصال والتي تشكل أهمية للاقتصاد الدولي وللبنية التحتية الكونية للمعلومات، حيث لا تختلف شبكات المعلومات عن أي مشروعات بنية تحتية أخرى تحتاجها أي دولة، والتي قد يكون لدول أخرى دور فيها بما يمثل انتهاك للسيادة الوطنية بمفهومها التقليدي، حيث أصبح للدول دور في البنية التحتية لدول أخرى مع زيادة الاعتماد المتبادل بين دول العالم في تقديم خدمة الإنترنت، و تبادل مقدمي خدمة الإنترنت البيانات مع منافسيهم المحليين والدوليين.

وعلى الرغم من أن الولايات المتحدة كانت مسئولة عن ٧٠ في المائة عن تبادل البيانات عن طريق الإنترنت قبل عقد، فإنه يتوقع أن تقل تلك النسبة لتصل إلى ٢٥ في المائة. بما يشير إلى تراجع الولايات المتحدة كنقطة مركزية في مجال خدمة الإنترنت ، وأصبحت الإنترنت تمثل ميزة تنافسية للولايات المتحدة، ولكنها أخذت تنمو خارج سيطرة الشركات الأميركية. وتشهد الشبكات الدولية التي تنقل البيانات داخل وخارج الولايات المتحدة توسعات بمعدلات كبيرة، ولكن البنية التحتية لخدمة الإنترنت في الكثير من المناطق الأخرى في العالم، تشهد نموا مطرداً وبصورة أسرع. وتوجه خدمة تبادل البيانات عن طريق الإنترنت إلى خارج الولايات المتحدة.

ولم تصبح الدول هي من يقدم فقط الخدمات كالأمن والتعليم والقانون والصحة وغيرها مع انتشار الخصخصة والسوق الرأسمالي. وعلى الرغم من ذلك لم يشهد العالم اختفاء دور الدولة القومية بل إنما يشهد حالة من تداخل السلطات وأصبح على الدولة أن تقوم بوظائفها في ظل ظروف التغير السريع للبيئة

الدولية، ومازالت الدولة تستطيع أن تفرض نفوذها على الواقع من خلال أيضا استخدام تلك الأدوات التي ساهمت في إضعافها حيث يتم استخدام الفضاء الالكتروني في الترويج لسياستها وشن الحملات الدعائية واستخدام ما وفرة من تقنيات في مجال القوة العسكرية، ومن ثم فان قوة الدولة لم يتم تقويضها مقابل قدرتها على ممارسة مظاهر سيادتها داخل الفضاء الإلكتروني[1].

و كشفت في الوقت نفسه أهمية الدور الذي يمكن أن تقوم به الدول كمفاوض أساسي في مجتمع المعلومات العالمي وإدارة الدبلوماسية الدولية عن طريق التفاعل مع العديد من الفاعلين واقامة شبكة التحالفات حول العالم، وأصبحت مسألة الحفاظ على البنية التحتية الكونية للمعلومات تدخل ضمن أولويات سياسات الأمن القومي للدول، وظهر ذلك في السعي لاستغلال الفضاء الالكتروني للحصول على مزايا في المجال العسكري وفي نفس الوقت العمل على حماية بيئة المعلومات الدولية.

وخاصة بعد أن أصبح النشاط الاقتصادي للدولة يتجه للاعتماد على القطاع الخاص بما أثرعلى وظائف الدولة وعلاقتها بمواطنيها وفقدت الدولة دورها التقليدي كفاعل مركزي في العلاقات الدولية وأفسح ذلك المجال أمام فاعلين آخرين ليكون لهم النفوذ والدور، بل أصبحت الدولة ذاتها بحاجة إلى إعادة تعريف دورها ووظائفها، بما أثر على أنماط الفاعلين في العلاقات الدولية، فظهر دور المنظمات الحكومية الدولية وأصبح بإمكانها اختراق حدود الدول والقيام بوظائف الدولة التقليدية بنجاح بما أدى لانتقال المسئولية من الدول إلى المنظمات الحكومية الدولية، وزيادة دور الشركات متعددة الجنسيات.

وعملت تكنولوجيا الاتصال والمعلومات على تمكن تلك المنظمات والشركات الدولية من زيادة دورها على المستوى الدولي وتمكنها من الوصول لعدد هائل من البشر والأعضاء من كافة دول العالم، و كما أدت قلة تكلفة إنشاء المنظمات غير الحكومية لانتشارها بالاعتماد عى الفضاء الالكتروني ، وأثر ذلك على إمكانية التحول من منظمات مادية إلى افتراضية تقدم الخدمات الكترونيا وتتصل بمستهدفيها بما يجعل من المنظمات أكثر فاعلية،

و أصبح لدى الأفراد القدرة على التحليل والنقد والمتابعة عبر الفضاء الالكتروني بما يؤثرعلى الرأي العام والضغط على الحكومات، وأصبح لهم دور في إنتاج المعرفة وتداولها عالميا والاتصال فيما بينهم عبرإنشاء تجمعات الكترونية داخل الفضاء الإلكتروني،ولا تعتمد على اقامتها داخل حدود إقليم معين أو هوية محددة أو لغة أو عرق أو نوع، وتتكون تلك التجمعات الالكترونية دون الأخذ في الاعتبار أي عوامل تمييزية في تكوينها ، ويتم التفاعل بين تلك التجمعات مع غيرها عالميا دون المروربمؤسسات الدول الرسمية.

وأصبحت العلاقة بين التكنولوجيا والمجتمع الدولي ذات طبيعة متبادلة حيث تصبح التكنولوجيا لها دور في تغيير قيم المجتمع الدولي مع قلة تأثيره على التكنولوجيا، ويكون له دور في التأثيرحين يتم توظيف التكنولوجيا لخدمة قيمه ومصالحه، ويعد الفضاء الالكتروني وسيلة إعلام دولية تستطيع أن

[1] Andreas Wenger ," The Internet and the Changing Face of International Relations and Security", Information & Security, an international journal ,ProCon Ltd., Sofia,Bulgaria ,Volume 7,2001, pp 5-11.

تحدث تحولات في الفكر الإنساني والتنظيم الاجتماعي إلا إذا كانت في حد ذاتها تعبيرا وانعكاسا لقيم ونظم اجتماعية محددة حيث يتم التزاوج ما بين القيم المحلية والعالمية والثقافات والأديان المختلفة.(1)

واصبحت المشاكل ذات الطابع الإنساني تجتذب اهتمام الرأي العام الدولي مع انتشارها السريع عبر الصوت والصورة والنص في الفضاء الإلكتروني، ووصولها لكافة أرجاء العالم دون أي عوائق بما يشكل في الوقت ذاته ضغطا من قبل الرأي العام المحلي على الحكومات لتغير سياستها بما يؤثر بشكل كلي على النظام الدولي، وأثر هذا من جانب في تقليل قوة الدول الكبرى نسبيا لصالح الدول الصغرى والفاعلين من غير الدول، وأصبحت العلاقات الدولية أكثر تعقيدا وتشابكا، وعلى الجانب الأخر ساعدت الثورة التكنولوجية في اتساع الفجوة بين من يملك تلك المقدرات وبين من لا يملك بما يساعد على ممارسة الهيمنة مع وجود فجوة بين دول الشمال والجنوب وبين الجنوب والجنوب وفي داخل الدولة ذاتها.(2)

أما فيما يتعلق بالقوة داخل النظام الدولي فان ثورة المعلومات قد أوجدت مزايا متباينة ومختلفة بين دول العالم في مجال قدرتها على إنتاج المعلومات وتراكم المعرفة ومدى ارتباطها بمجتمع المعلومات الدولي، وأصبحت المعلومات مصدراً هاماً من مصادر القوة، وأدى التفاوت الدولي في الحصول عليها لصعوبة استيعاب سوق العمل للبطالة المتعلمة بما يؤدي لحدوث اختلالات اجتماعية تشكل بيئة لبروز الجريمة والعنف في ظل صياغة التفاوت الاقتصادي أو السياسي على نحو ثقافي أو عرقي أو طائفي، و تكريس الانقسام بين أقلية تمتلك القدرة على النفاذ إلى الإنترنت وأغلبية لازالت تفتقد تلك القدرة والتي تعني الحصول على الثروة والسلطة .

وهو ما يؤدي بدوره إلى تعميق الأزمات الاجتماعية داخل المجتمع في ظل عدم استقرار سياسي في إطار مشكلات الانتقال أو التحول الديمقراطي وما سيتبعه من عملية تفكيك للدولة كون إن العامل التقني يؤكد على الهويات والانتماءات الأولية وطرح الفضاء المعلوماتي تأثيرات على الهوية فلم تعد يتم تشكيلها محليا ، وعمل الإنترنت على تشكيل وإعادة الجماعات والهويات ووضع أسساً جديدة يكون للفرد دورا فيها وليس بالضرورة للجماعة التي يتمنى اليها الفرد دوراً في صياغتها ، وظهرت عملية بناء هويات بدون أجساد من خلال إضعاف الهوية التقليدية وتغيير الجذور التي تقام عليها (3).

(1) Shorer-Zeltser, M. and Ben-Israel, G. M. Religious Internet Networks and Mobilization to Terror. Journal of Information Warfare No.6 ,August 2007.pp:1-14.

(2) د. حسن مظفر الرزو، "الفضاء المعلوماتي" ، مرجع سابق ذكره،ص ص ٣٠٥-٢٥٤.

(3) Kath Wood ward, "**Understanding Identity** " chapter 5"emboding identity ", Oxford university press inc. 2002,pp103-133.

# المبحث الثاني:
# الطابع الالكتروني للقوة والدبلوماسية والصراع في النظام الدولي

**يتكون هذا المبحث من محاولة الباحث استعراض طبيعه التغير في القوة والصراع وخاصة على النحو الايجابي بالنسبة الى الصراع من خلال الدبلوماسية الالكترونية او من خلال ظهور قوة المعلومات والاقتصاد الرقمي الجديد الذي شكل نمو الاقتصاد الدولي ، وياتي هذا على الترتيب من خلال ثلاثة مطالب ، ياتي الاول بتناول ثورة المعلومات والتحول في القوة في العلاقات الدولية ، واما المطلب الثاني فيتناول الفضاء الالكتروني وظهور نمط القوة الالكترونية اللينة ، واما الثالث فيتناول الدبلوماسية الالكترونية وحل النزاعات الدولية.**

## المطلب الاول:

## ثورة المعلومات وتحول القوة في العلاقات الدولية

تعرف القوة بصفة عامة بانها القدرة على التاثير في سلوك الاخرين للحصول على نتائج محددة يريدها احد الاطراف الذي يمارس القوة ضد الطرف الاخر، ومعنى القوة في المفهوم السياسي هي القدرة على تغيير سلوك اجتماعي معين، ويعرف هانس مورجانسو القوة بانها القدرة على التاثير في سلوك الاخرين او تغييرة وفق الاتجاه المرغوب به من جهة ومن جهة اخرى القدرة على مقاومة محاولات الاخرين للتاثير في السلوك والمصلحة هي جوهر العمل السياسي وهي تتحدد بمؤشر القوة.

وتكون القوة وفق العديد من التعريفات هدف في حد ذاته بالنسبه الى الدول او قد تكون كاجراء من اجراءات النفوذ او السيطرة على النتائج والاحداث والجهات الفاعلة في القضايا المختلفة، وقد تكون القوة تعكس الانتصار في الصراع وتحقيق الامن ، او تعني السيطرة على الموارد والقدرات ،اذا كانت القوة تعني القدرة على التاثير في الاخرين لدفعهم لفعل ما تريد وذلك من خلال ثلاثة طرق رئيسية لتحقيق ذلك الاولى عن طريق التهديد بالفعل المادي او الضرب والطريقة الثانية عن طريق دفعهم بالمكافأه اما الطريقة الثالثة من خلال اجتذابهم .

وهي تلك القوة الناعمة او اللينة وهو اصطلاح جديد طرحه جوزيف ناي ، والذي يرى ان القوة العسكرية والاقتصادية وكلاهما يطلق عليهما(القوة الصلبة ) لم تعد كافية في الهيمنة او السيطرة لذا فهو يدعو الى استخدام قوة غير عسكرية في الترويج والترغيب للافكار والسياسات حيث يتم جذب الاخرين ولا يتم اجبارهم على التغيير من خلال التهديد او استعمال القوة العسكرية او الاقتصادية. والقوة الناعمة ليست تماماً كالتأثير، مع انها مصدر من مصادر التأثير المتعددوهي تعتمد اكثر من الاقناع والبرهنة بالجدل، فهي الاغراء والجذب غالباً ما تؤدي الى الرضوخ والتقليد[1] وتوجد للقوة الناعمة انماط او اشكال مختلفة منها القوة الاقتصادية المتمثلة في المساعدات المالية او فرض

[1] Joseph S. Nye, Jr., The Decline of America's Soft Power, Foreign Affairs, May/June 2004.

العقوبات اقتصادية ، وهناك القوة الثقافية حيث ترتكز على قدرة الدولة على الحصول على ما تريد من نتائج واهداف وذلك بسبب تاثيرها الثقافي والقيمي على الاخرين ، وهناك صلة بين القوة الناعمه والقوة الصلبة لان كلاهما يمتلك القدرة على تحقيق هدف واحد من خلال التاثير على الاخرين، فالقوة المرنة تساعد على تشكيل اتجاهات وسلوك الاخرين للقيام ما يريدة من يمتلك تلك القوة استنادا الى القيم والثقافة ، وترتبط القوة الصلبة اكثر في عملية استخدامها بسلوك القايدة السايسية صانعي القرار،وقد كان لثورة المعلومات والاتصال تاثيرا كبيرا على القوة الناعمة حيث انها اتسعت ولم تعد تشمل وفق تعريف جوزيف ناي المساعدات او العقوبات الاقتضادية .

يبرز الجدول رقم (١) مدى تأثير تكنولوجيا المعلومات على القوة[1]

| تأثير تكنولوجيا المعلومات على القوة◆ | | |
|---|---|---|
| القوة المرنة | القوة الصلبة | الأطراف |
| توسيع دائرة الإنتاج ودفع النمو الاقتصادي<br>فرص للهيمنة وتسويق القوة | الثورة في الشئون العسكرية<br>الاستثمارات الضخمة في التقنية<br>فرصة اللاعب الأول والتأثير في الهيكل | القوى الكبرى |
| تسهيل عملية التفاعل لدى المنظمات الدولية<br>تقليل حجم الاعتماد على الخاص وإنشاء مجتمعات افتراضية | الإمكانيات التجارية<br>تدعيم البنية التحتية<br>دعم المجال الاقتصادي والتجاري والأسواق | القوى الصغرى |

وانقسم تأثير تكنولوجيا الاتصال والمعلومات على القوة بنوعيها الصلب والمرن، فتتعلق القوة المرنة داخل القوى الكبرى بأنها تساهم في توسيع دائرة الإنتاج ودفع النمو الاقتصادي وتتيح الفرصة للقوى الكبرى أن تمارس هيمنتها على النظام الدولي، أما بالنسبة للقوى الصغرى في النظام الدولي فان تكنولوجيا الاتصال والمعلومات تساعدها في عملية التفاعل لدى المنظمات الدولية وتقليل حجم الاعتماد على الأشخاص وإنشاء تجمعات الكترونية وبناء تحالفات دولية.أما فيما يتعلق بالقوة الصلبة وعلاقاتها بتكنولوجيا الاتصال والمعلومات فإنها تساعد القوى الكبرى على إحداث ثورة في الشئون العسكرية والقيام بالاستثمارات الضخمة في مجال التقنية وإعطائها الفرصة لتكون اللاعب الأول والمؤثر في هيكل القوة داخل النظام الدولي، أما بالنسبة للقوى الصغرى فان دور تكنولوجيا الاتصال والمعلومات يقتصر على دعم إمكانياتها التجارية والبنية التحتية والمجال الاقتصادي ويأتي هذا مع زيادة أهمية العلم والتكنولوجيا والتي أصبحت ظاهرة أكثر ارتباطا بالعصر الحديث، وأصبح هناك ارتباط وثيق بين التكنولوجيا والأغراض المدنية والطبية والخدمية وغيرها إلى جانب دور التكنولوجيا في الجانب العسكري فيما يتعلق بدورها في التأثير على طبيعة ونوعية الأسلحة وقدرتها التدميريه، وعمل هذا التطور ثنائي الاستخدام للتكنولوجيا على إحداث تغير في مصائر الدول وقدراتها القتالية وميزانها

(1) Richard K.Betts,(editor), Robert O. Keobane & Joseph S Nye ,**"Power ,Interdependence, And The Information Age "**, at ," conflict after the cold war :arguments on causes of war and peace ", Second Edtion ,2002 ,pp 548-557.

العسكري وقوتها النسبية مع غيرها، وقدرتها على السيطرة والنفوذ والثروة وارتباط ذلك بأهمية دورالقوى البشرية.[1] وأصبحت المعلومات قوة قومية وأداة من أدوات حروب المستقبل وساحة يتصارع فيها الأعداء وكانت إحدى ساحات المواجهة تلك الفضاء الالكتروني سواء عبر استغلالها من قبل الجماعات الإرهابية أو استخبارات الدول المعادية لبعضها البعض، بعد أن تحولت لشبكة عالمية وتمتعها بمزايا كرخص التكلفة وسهولة انتقال المعلومات والأخبار عابرة الحدود وتجاوز العوائق الأمنية التقليدية ،وأصبح للفضاء الالكتروني دور في إحداث الحراك الاجتماعي والسياسي على المستوى المحلي والدولي، ووجود درجة عالية من التفاعل والاعتماد المتبادل بين دول العالم ،ووجود رابط اقتصادي وامني مشترك بينها .

وساهمت ثورة المعلومات في تغير ثوري في شن الحرب ووسائلها، ولم يأت ذلك فقط من جراء السباق التكنولوجي بل جاء أيضا من تبني الطرق والوسائل العسكرية لتحقيق الأغراض السياسية ،وخاصة مع زيادة البعد الثقافي والديني في العلاقات الدولية، وأثرت ثورة المعلومات في مقاييس القوة ومعاييرها ومصادرها وانماطها وانتشارها، وبما اثرعلى كافة اشكال القوة بمعناها الشامل، والتي من أهم مظاهرها ثلاثة أنواع قوة عسكرية وأخرى سياسية واقتصادية، و تعني القوة السياسية بقدرة الدولة على تحقيق أهدافها، أما الاقتصادية فتعني قدرة الدولة على الحصول على الموارد والمواد الخام، أما القوة العسكرية فكانت ترتكز على قوة الجيش الكمية، وأصبحت السيطرة على المعرفة والمعتقدات والأفكار ينظر إليها باطراد كبداية للسيطرة على الموارد مثل القوات المسلحة والمواد الخام.

واصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم ، والتي تشمل الطاقة والاتصالات والنقل والخدمات الحكومية والتجارة الالكترونية والمصارف والمؤسسات المالية، وحيث جعل الفضاء الإلكتروني من تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة والتي تعرف بالبنية التحتية القومية للمعلومات (NII) ومن ثم فان أي هجوم على إحدى تلك المصالح أو كلها يمثل سببا ومدعاة لحدوث عدم توازن استراتيجي بما يكشف في الوقت نفسه عن شكل جديد من أشكال الصراع.[2]

وأدت ثورة المعلومات لقيادة التغير في هياكل القوة وسيادة الدول بما أثر على مفاهيم الأمن وطبيعة الفاعلين و مصادر القوة التي تتحول من الطابع العسكري للاقتصادي الى مصادر المعلومات، و أدى ذلك لانتقال السلطة من المركز إلى إعادة توزيعها داخل المجتمع الدولي، وزادت القوة داخل المجتمعات المحلية من جراء إسهامها في الثورة التكنولوجية وقدرتها على الإنتاج المعرفي والمساهمة في مجتمع المعلومات العالمي، وأصبح لشبكات المعلومات والاتصال دور في القوة العسكرية سواء بالاستخدام المباشر أو غير المباشر[3]

[1] Jeffrey C. Sobel, **Digination: The Birth of Cyber-Nations.** Maxwell AFB, AL, Air Command and Staff College, 2005. p 30.
[2] Richard K.Betts, (editor), **"conflict after the cold war: arguments on causes of war and peace "**, second edition, 2002, pp 548-557.
[3] James R. Blaker,. **Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare.** Westport, CT, Praeger Security International, 2007. pp 248.

## المطلب الثاني:

## الفضاء الالكتروني وظهور نمط " القوة الالكترونية " اللينة"

تعرض العالم المعاصر لعدد من المتغيرات كان من أهمها تنامي ظاهرة العولمة، والتي كان من اهم أدواتها التكنولوجية شبكة الإنترنت وتكنولوجيا الاتصال والمعلومات والتطور الهائل في وسائل الاتصال والإعلام، وأدت هذه الثورة لتحويل العالم في جزء منه من الطابع المادي "Real World" إلى عالم رقمي وافتراضي "Virtual" [1]، وانتقلت كافة مجالات الحياة لتأخذ طابعا رقميا يدور في فلك الفضاء الإلكتروني،

ولم يسهم فقط انتشار تكنولوجيا الاتصالات الحديثة، مثل الإنترنت والإعلام العالمي في تجاوز الحدود، وإنما أسهم كذلك في إرباك الثقافات السياسية التقليدية و القائمة على الطاعة العمياء للنظام الحاكم من قبل المواطنين في مقابل دور الإنترنت في تعزيز عملية تشكيل الشبكات الأفقية وتحرير الاتصالات ودعم ثقافة النقاش المفتوح. مما أدى إلى الوقوف ضد الثقافات السياسية التي تتسم بالتراتبيه والسيطرة من الأعلى التي لا تزال قائمة في بعض بلدان العالم.

وظهرت أشكال متنوعة من الاتصالات تتجاوز الحدود القومية للدول، وجاء ذلك في إطار ما يطلق علية " إعلام العولمة " والذي يعني " التعظيم المتسارع والمذهل في قدرات وسائل الإعلام والمعلومات على تجاوز الحدود السياسية والثقافية بين المجتمعات بفضل ما تقدمه التكنولوجيا الحديثة مع التكامل والاندماج بين هذه الوسائل، و يمثل الإعلام العولمي آلية أساسية للعولمة الاقتصادية باعتبارها تيسر التبادل الفوري واللحظي للمعلومات وتوزيعها على المستوى الكوني، وأصبح الطابع الدولي للمعلومات له دور في خلق أشكال جديدة من التضامن والتعاون بين الأفراد عبر الشبكات الدولية من اجل تحقيق أهداف وقيم مشتركة. [٢]

وأصبحت القوة الالكترونية cyber power حقيقة أساسية في العالم بكل مظاهرها المتنوعه وبما عمل على دعم ومساندة العمليات الحربية والقوة الاقتصادية والسياسية، ودور ثورة المعلومات والمعرفة في بروز مجتمع المعلومات الدولي والاقتصاد الالكتروني الجديد الذي أثرعلى طبيعة النظام الدولي فيما يتعلق بالتقسيم الدولي للعمل، وهو الذي يحدد آفاق النمو أمام مختلف البلاد، ويعمل أيضا على توزيع الموارد الاقتصادية ومستويات النمو الاقتصادي، وأنماط التفاعل بين القوى الاقتصادية الدولية، والتأثير على القوة السياسية بالتأثير على عمليات صنع القرار في النظام الدولي.[٣]

(1) يفضل الباحث استخدام كلمة "الرقمية أو الالكترونية بدلا من كلمة" الافتراضية " حيث يرى الباحث أن الكلمة الأخيرة تعني افتراض وجود شيء ما وتحمل مدلول انه قد لا يوجد، ولكن في الواقع إن الفضاء الالكتروني هو وسيط موجود فعلا وواقعيا ويتلمسه الناس ودخل في كافة مجالات الحياة.

(2) أدهم عدنان طبيل، " الإعلام الحديث في ظل العولـمة": ٢-٠٥-٢٠٠٧ يمكن الاطلاع علية على الرابط التالي (اخر زيارة ٢-٨-٢٠٠٨ ) (http://pulpit.alwatanvoice.com/content-89911.html)

(3) عادل عبد الصادق، " مصر ومجتمع المعلومات: هل يمكن تكرار التجربة الهندية ؟" مجلة تطبقات مصرية، مركز الدراسات السياسية والاستراتيجية بالاهرام العدد ١٧، ١٨ يوليو ٢٠٠٤.

وساعد ظهور الفضاء الالكتروني على زيادة الدور النسبي للقوة الناعمة في العلاقات الدولية اما في شكل المعلومات والتاثير على القيم والراي العام بما يظهر في شكل تغير في السلوك او عن طريق ووجود اسلحة جديدة ذات طابع الكتروني تدور عبر الفضاء الالكتروني وتعتمد على المعلومات والابتكار والذكاء البشري .ويتمتع هذا الشكل الجديد من القوة الناعمة بخروجة عن سيطرة الحكومات حيث ان الفضاء الالكتروني عابر للحدود ومتاح لاستخدامة من قبل أي فرد.

وأصبح امتلاك القدرة على المساهمة في الثورة المعلوماتية يمثل مفاتيح القوة في العلاقات الدولية، وأصبح يمثل مجالاً لهيمنة الدول بعضها على بعض سواء بطريقة مباشرة عن طريق السيطرة والتحكم في المقدرات أو بطريقة غير مباشرة عن طريق القدرة العالية على زرع عملاء في الأجهزة التنفيذية واستخدام تكنولوجيا الاتصال والمعلومات والتقدم التكنولوجي في التجسس. وتحولت القوة العسكرية من قوة النيران إلى قوة المعلومات ثم إلى قوة الذكاء البشري.[1]

وتستخدم الدول الفضاء الإلكتروني لاعتبارات الأمن والقوة العسكرية بشكل جعل العديد من الدول تدخل الفضاء الالكتروني ضمن حسابها الاستراتيجي واستراتيجية القومية للامن، وهذا الى جانب دور الفضاء الالكتروني في تحقيق الرفاهية الاقتصادية والحصول على موارد الثورة والسلطة وتحقيق التفوق السياسي، وتعظيم معرفتها وسباقها العلمي والبحثي والقدرة أيضا على تحقيق السلم والأمن والتفاهم الدولي من خلال دور الفضاء الإلكتروني كأداة اتصال ووسيلة إعلام دولية.

وذلك عن طريق دورها في الكشف السريع عن مكونات الدولة السياسية والاقتصادية والثقافية عبر ما يتم تداوله من معلومات في الفضاء الإلكتروني، وتوفير مادة هامه لاستخدامها من قبل الخصوم والأعداء، وهذا إلى جانب ما يتم أتاحته من صور فضائية لمكونات البنية التحتية الداخلية للدولة التي يوفرها برنامج مثل جوجل أيرث " بالإضافة إلى خدمة البث المباشر لما يجري في شوارع أو مداخل المدن الكبرى للدولة، هذا إلى جانب إمكانية تسليط البرنامج على معسكرات اللاجئين أو قضايا عالمية أخرى يمكن رؤيتها عن قرب، وطرح ذلك مدلولات جديدة للأمن الدولي، بالإضافة إلى إمكانية نشر صور أو معلومات تعتبر سرية أو عسكرية ونشرها في المواقع ذات الطبيعة الاجتماعية والتي تلقى إقبالاً كبيراً من الناس في كافة ارجاء العالم ،والتي تسري في اتجاه تبلور دليل إلكتروني عالمي يحتوي على أكبر قدر ممكن من المعلومات والتفاصيل الشخصية للأفراد مثل المواقع الاجتماعية على الإنترنت والتي تلقى إقبالاً كبيراً من الملايين حول العالم.

وهناك تطور تكنولوجيا تلك المواقع كحال برنامج"Sky" الذي يتيح للمستخدمين ملاحظة ومراقبة الكواكب والأجرام السماوية ويشكل يعكس مدى التداخل ما بين الفضاء الخارجي والالكتروني. وأتاحت تلك المعطيات الاستراتيجية الفرصة لاستغلالها من جانب الفاعلين في المجتمع المعلوماتي العالمي في التجنيد والحشد والتعبئة والتنسيق وجمع المعلومات لتنفيذ عمليات عدائية بمساعدة الفضاء

(1) David C. Gompert, Irving Lachow,and Justin Perkins," **Battle-Wise Seeking Time-Information Superiority in Networked Warfare**"Center for Technology and National Security Policy, National Defense University Press, Washington, D.C.,2006,pp 3-13.

الإلكتروني، وكونه ايضا وسيلة اعلام دولية تتميز برخص التكلفة وسرعه الانتشار والطابع الفردي له، و بما يشكل ذلك ضغوطا متزايدة على صانعي القرار وهدد بدوره الاستقرار داخل المجتمعات، وفرض تحديات داخلية وخارجية للأمن الدولي.

وظهرت العلاقة ما بين الفضاء الالكتروني والأمن الدولي حيث يوجد المحتوى المعلوماتي العسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي في الفضاء الإلكتروني، خاصة مع التوسع في تبني الحكومات الالكترونية من جانب العديد من الدول، واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجي، وهذا مما يعرضها لخطر التعرض لهجمات الفضاء الالكتروني الى جانب الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لإعمال تحريضية أو دعم المعارضة الداخلية للنظام الحاكم ور تقديم الدعم المادي والمعنوي عبر الفضاء الإلكتروني.

ويستخدم الفضاء الإلكتروني في القيام بحروب غير تقليدية [1] عبر هجمات الإرهاب الإلكتروني و إطلاق فيروسات الحاسب والتجسس الالكتروني والاختراق المباشر لشبكات المعلومات، ولم تعد أشكال الخطر التي تهدد المحتوى المعلوماتي والمجتمعي المشترك مقصورة على الأشكال التقليدية بل أصبح لها أوجه رقميه الكترونية غير مسبوقة في شمولها وعمقها واختلافها واتساع نطاق تغطيتها وفداحة أضرارها وذكاء منفذيها وتعقد آلياتها وتواصل هجماتها وتتضمن أخطارتعقب وجمع المعلومات والثانية تقوم على إفساد وتعطيل إتاحة المعلومات مثل المعلومات العسكرية والأمنية والاقتصادية والمحتوى الفكري والسياسي والاجتماعي والعلمي.[2]

ومن ثم تصبح تلك المعلومات عرضة للتوظيف لتصبح أداة في يد الجماعات الإرهابية أو أجهزة التجسس الدولية والجريمة المنظمة وغيرها من الفاعلين ممن يجد له مصلحة في الاستفادة منها أو ضرب نظام عملها، وهذا يعكس تطور مفهوم الأمن القومي تجاه التهديدات الجديدة غير التقليدية والتي قد تكون نابعة من داخلها أو واقعه تحت سطوته من الخارج، واتساع مجال الأمن ليمتد من الجانب العسكري لمجالات أخرى عديدة وشملت تهديدات خارجية وداخلية وتداخلاً لقطاعات التهديدات وفي مستوياتها. [3]

وتعمل أجهزة الحكومة الإلكترونية في العالم فضاء مفتوح يتداخل فيه جمهورها الخارجي من المواطنين، مؤسسات، حكومات أخرى) مع جمهورها الداخلي (وزراء، موظفون...) وتصبح فيه أجهزتها عرضة للعديد من الاخطار تحت دوافع مختلفة، ومن الممكن أن تتم مهاجمة أنظمة الحكومة الإلكترونية من داخلها وعبر أحد الموظفين الغاضبين أو من الخارج عبر مجموعات الهاكرز أو أجهزة

[1] L. Walsh. and J. Barbara," Speed, international security, and "new war" coverage in cyberspace". Journal of Computer-Mediated Communication, 12(1), Article 10. (2006) (http://jcmc.indiana.edu/vol12/issue1/walsh.html)

[2] جريدة الأهرام ٧ فبراير - ١١ ابريل ٢٠٠٦.

[3] د.بهجت قرني "تراكم الانكشاف الاستراتيجي العربي وأهمية البعد الثقافي المهمل"، مجله المستقبل العربي، مارس ٢٠٠٢، " مركز دراسات الوحدة العربية، بيروت، ع ٢٧٧ ،ص ٥٤-٦٩.

الاستخبارات في بلدان معادية وصولاً إلى المؤسسات التجارية الساعية إلى الحصول على معلومات تجارية تنافسية. ومن الممكن أن تعمد أجهزة المخابرات الصديقة أو المعادية على حد سواء للحصول على المعلومات عن أشخاص أو مؤسسات أو حتى أجندات الحكومة الداخلية عبر تنفيذ هجمات الكترونية بهدف اختراق النظام الأمني المعلوماتي للحكومة والدخول إلى مختلف الأنظمة بها، وقد توظف أجهزة المخابرات في هذه العملية كفاءات تقنية عالية وقادرة في كثير من الأحيان على اختراق أنظمة الحكومة محل الهجوم وفرض الفضاء الإلكتروني كذلك تحدياً ذو طابع مرن يتمثل في الغزو الثقافي للدول الأخرى والترويج لثقافة عالمية مهيمنة جديدة.

ويستخدام الفضاء الالكتروني من قبل الجريمة المنظمة والجماعات الارهابية وتجارة المخدات وغسيل الاموال وتسهيل نشاط كافة انواع الجرائم و الأنشطة التي تهدد امن واستقرار الدولة، والعمل على تهديد الاستقرار الاقتصادي للدول من خلال نشر الموضوعات الدعائية المغرضة وإساءة استخدام بطاقات الائتمان، وكذلك الإساءة إلى سمعة الدول والشركات والأفراد والماركات التجارية من خلال الإعلانات الهدامة التي تنشر وتذاع مستهدفة الماركات المنافسة أو الدول المنافسة بالإضافة إلى إساءة التعامل مع حقوق الملكية الفكرية للأعمال الفنية والمؤلفات العلمية وقواعد البيانات والموسوعات وغيرها من المصنفات الفنية ، والعمل على الإساءة لكرامة الإنسان خاصة الأقليات واستخدام الإنترنت كوسيلة للتمييز العنصري بالإضافة إلى مضامين تسهيل الجريمة المنظمة وتجارة المخدرات والجنس وغسيل الأموال وأوجدت الثورة التكنولوجية أطرافاً وفاعلين جدداً، وأصبح لديهم القدرة على التأثير والنفوذ أكثر من غيرهم وذلك عن طريق، ولم يواكب تنامي دور الفضاء الالكتروني على الصعيد الدولي وجود نظام قانوني دولي ينظم العلاقات والتفاعلات داخل النظام الدولي بما مثل ذلك تحديات لسيادة وأمن الدول و البناء الوظيفي للنظام الدولي.

## المطلب الثالث:

## الدبلوماسية الالكترونية وحل النزاعات الدولية

١- تغير بيئة ومحيط العمل الدبلوماسي

جاءت التغييرات في النظام الدولي بانهيار الاتحاد السوفيتي وانتشار موجة الديمقراطية في العالم الثالث والانتشار الواسع لتكنولوجيا الاتصال والمعلومات منذ منتصف التسعينات لتشكل جميعها مدخلا جديدا للعلاقات الدولية ،وما فرضته من تداعيات وآثار وطرق حل للمنازعات الدولية والصراع، وأصبح هناك توجه عالمي للاهتمام بقضايا عالمية كتغييرات المناخ وحقوق الإنسان واللاجئين والهجرة غير الشرعية ومناطق النزاع المسلح في العالم.

وبرزت حاجه البشرية إلى زيادة الاهتمام بالسلام ومعالجة أية خلافات عن طريق الحوار والتفاوض بدلا من استخدام العنف والحرب، وذلك بعد أن كان النظام الدولي التقليدي يعتمد على النظام ذي الطابع الدولي أي علاقات الدول ببعضها البعض مباشرة على المستوى الرسمي، ووجود نظام دولي وسيط يتمثل في المنظمات الدولية، أصبح يتجه مباشرة للاعتماد على الشبكات الاتصالية الدولية،

وأصبح التفاعل يمكن أن يتم على مستويات محلية بين الدول، مع ظهور تحديات حول سيادة الدولة وتغير طبيعة الأمن والقوة في العلاقات الدولية التي كانت من مرتكزات العمل الدبلوماسي التقليدي.(١) وأصبح لتكنولوجيا الاتصال والمعلومات دور متصل ومتواصل مع دوائر صنع السياسة الخارجية وخاصة فيما يتعلق بإدارة الصراع الدولي وتسوية الصراعات، وتصاعد الاعتماد المتبادل بين التكنولوجيا والسياساتوظهر ذلك في كافة المجالات بدءاً من التعليم والصحة ونهاية بالحكومة الالكترونية، وكان من ضمن تلك الهيئات الحكومية وزارة الخارجية أو الوزارات المعنية بإدارة العلاقات الدولية، وكان لذلك تأثير واضح على طبيعة وبيئة العمل الدبلوماسي، وكذلك على الكادر الدبلوماسي وتغير طبيعة ودور الدبلوماسية وقضاياها، وظهور فاعلين جدد في صنع الدبلوماسية. وإلى جانب الدبلوماسية الرسمية التي تعبر عن سياسة الدولة الخارجية جاءت أشكال أخرى مستفيدة من انتشار تكنولوجيا الاتصال والمعلومات المتسارعه عالميا والذي جعل العالم بمثابة قرية صغيرة، وزادت أهمية الدبلوماسية الشعبية ودور الفاعلين من غير الدول في التأثير في صنع قرارات السياسية الخارجية للدول.(٢)

وأفضت الثورة التكنولوجية تغيير في أسس العمل الدبلوماسي، وظهر دور لفاعلين جدد ولم تعد الدولة هي الفاعل الوحيد في العلاقات الدولية، واختلف معيار القوة بتحوله من القوة التقليدية التي تعتمد على عناصر القوة القومية المرتكز على السكان والموارد والجيش لمفهوم القوة التي تعتمد على تكنولوجيا الاتصال والمعلومات، وأثرذلك على تغيير مناسيب القوة في العلاقات الدولية بالاعتماد على الاقتصاد الرقمي الجديد، والتي جعلت دولا صغيرة الحجم ولديها سكان اقل وموارد طبيعية محدودة يضاهي حجم الناتج الإجمالي للدول الكبرى ، ودفع التخصص في العمل لزيادة الاعتماد الدولي ،و برز مفهوم امن جماعي مشترك ذي بعد إنساني ،وزيادة قوة الرأي العام العالمي بما شكل في ذات الوقت قيوداً على صانعي القرار في الدول .

٢- ظهور مفهوم الدبلوماسية الالكترونية.

عمل الفضاء الالكتروني كوسيلة ووسيط جديد للعمل الدبلوماسي عبر الانترنت والمحمول والكمبيوتر والاتصالات عن طريق الأقمار الصناعية، وما يوفرة من معلومات جيوسياسية، وأثره على وظائف الدبلوماسية وهي الحماية لمصالح الدولة والملاحظة والمتابعة والمفاوضات وجمع المعلومات، والمشاركة في صنع القرار، واتاحت الفرصة لوضع نموذج لمحاكاة المنازعات الدولية وتعظيم فوائد التدريب ورفع كفاءة العنصر البشري عن طريق ما يمكن أن يتيحه الانترنت من مهارات لغوية ومعلوماتية وتفاوضية، ويمكن الإطلاع على كافة مناطق النزاع والصراعات، و إقرار مشروعات أمنية مشتركة بين الدول عن طريق مواقع الانترنت والتواصل مع الأطراف المعنية من خلالة.

(1) Richard Solomon," **The Global Information Revolution and International Conflict Management**", United States Institute of Peace, virtual diplomacy report , VDS No. 17,January 2004 . (http://www.usip.org/virtualdiplomacy/publications/papers/rhsvd.html)

(2) Sheryl J. Brown and Margarita S. Studemeister "Virtual Diplomacy: Rethinking Foreign Policy Practice in the Information Age ",Information & Security. Volume 7, 2001, pp. 28-44.

وتعرف الدبلوماسية بأنها كل علم يعنى بفن التفاوض، وتبرز كوسيلة أو أداة للتفاوض من اجل إقناع طرف أو أطراف، ولا يوجد تعريف محدد للدبلوماسية إلا أنها تجمع بين بعض السمات مثل أنها فن يصنع برامج السياسة، و فن إدارة العلاقات الدولية، وعملية إدارة المعاملات بين الدول بأساليب الحوار والتفاوض، باعتبارها لغة الحوار والنقاش والإقناع، وفن التعامل بين المنظمات الدولية وحل مشكلاتها وهي لغة العقل الهادئ لا الحرب والصراع، وتعمل على تحقيق ما تعجز آلة الحرب عن تحقيقه وتدخل في المجالات الاقتصادية والسياسية والإعلامية والثقافية، وتاخذ الدبلوماسية طابعها الالكتروني بعملية محاكاة للواقع الفعلي، فالدبلوماسية الافتراضية هي دبلوماسية حقيقية، تتم عبر وسائل تكنولوجية.

٣- دور الدبلوماسية الالكترونية .

اصبح للدبلوماسية الافتراضية دور في إدارة الصراع الدولي وذلك عن طريق دورها في اكتشاف كيف إن العالم أصبح في طور التغيير بتعرضه لثورة المعلومات العالمية، و استخدام التكنولوجيا الجديدة في عملية البيانات والمعلومات والاتصالات ،وذلك للمساعده في منع وتسوية الصراع والمصالحة أو إدارة الازمة ،والقدرة على أقامه تحالفات جديدة من الحكومات والمنظمات الدولية والمجتمع المدني والقطاع الخاص وحشد الرأي العام الدولي، والتنسيق الفعال بين أنشطتها وتوضيح حجم التحديات وتجاوز الحدود المكانية. ويشهد الفضاء الالكتروني عمل وتشكيل الشبكات الالكترونية والمجموعات والتجمعات الدولية، وقدرتة على تقليل الوقت والزمن وتجاوز الهياكل البيروقراطية للحكم ،و بناء روابط الكترونية بين المواطن وصانعي القرار بصفه مباشرة دون المرور بالضرورة عبر المؤسسات السياسية الرسمية، وفي إدارة الأزمة والصراع الدولي، والتي تتطلب وجود حماية لقنوات الاتصال بين الأطراف المتنازعة، وتوفير معلومات عنهما بسهولة والخروج عن سيطرة تقارير أجهزة الاستخبارات، وإمكانية وجود طرف ثالث محايد ،وإمكانية الاتصال المباشر بين الفرقاء، والتأثيرعلى التحالفات وطريقة صنعها وعلى المؤسسات واستراتيجيات المفاوضين.

وعزز الفضاء الالكتروني من التغيير الهيكلي للدبلوماسية بالانتقال الجزئي من الاعتماد على الدولة الرسمية إلى تفاعل جهات وجماعات وأفراد داخل الدول، والانتقال من مرحلة تبني النموذج التقليدي المركزي في صنع السياسة الخارجية للانفتاح على طرق تنفيذ أهدافها،وتم تنشيط الاتصالات الداخلية ووزارات الخارجية و الانفتاح على المعلومات، والتنسيق الفعال بين الأجهزة الحكومية بما يساعد على تقليل حجم النفقات.[1]

٤- خصائص الدبلوماسية الالكترونية:

- المركزية واللامركزية: بتنقية الجهاز البيروقراطي من الفساد وعرقلة القرارات وتقليل التكلفه وتوفير قنوات اتصالية سهلة داخل المنظمة ،وبشكل يقلل من الاعتماد على الإدارة الوسيطة أو الهرمية وجعلت القرارات أكثر سرعة للاستجابة لمتطلبات المجتمع بما يزيد من الكفاءة والفعالية .

[1] Amir Dhia," The Information Age and Diplomacy: An Emerging Strategic Vision in World Affairs", Published by Universal-Publishers, 2006 ,pp 120-428.

- التفتت والاندماج: بالتأثير على التنظيم الاجتماعي و إنشاء روابط وتجمعات الكترونية بين الدول المختلفة، بما يعزز من التفاهم الدولي المشترك، وكذلك تسهيل عملية اندماج المجتمعات المحلية في السياسة العالمية و إمكانية التنسيق لتشكيل راي عام دولي خلف القضايا المختلفة.

- الشفافية: اصبح العالم أكثر قربا من بعضه البعض عن طريق دعم التكتل وراء قضايا عالمية وجعلت ما يحدث في أي دولة يمكن معرفته في دولة أخرى كانتهاكات حقوق الإنسان وانتهاكات الحد من التسلح والديمقراطية والمحاسبة السياسية، و ساعد ذلك على حالة الشفافية في نشر المعلومات وما يكون لها دور في صنع القرار.

- التعبئة والرشادة: مكنت المعلومات من إمكانية تعبئة الرأي العام خلف ما يحدث ودفع الجماهير للقيام برد فعل قد يغلب علية الاستجابات العاطفية، والمساعده في الرشادة في اتخاذ القرارات بما ينعكس على إمكانية التورط في الصراع، وذلك من خلال وسائل الإعلام الجديد ،والموازنة بين التكلفة والعائد للصراع.

- السرعة: بتجاوز الزمان والمكان وقيود الجغرافيا وذلك بفعل الكمبيوتر والأقمار الصناعية وأنظمة الاتصالات بما ساعد في عمل المنظمات الإنسانية وعمليات حفظ السلام، وتوفير معلومات بصورة سريعه عن أماكن الكوارث والصراع والقضايا والأحداث العالمية ، وبما يعمل على تسريع الخطى لاحتواء الصراعات، وتسريع وتيرة التدخل الدولي في اطار الامن الانساني المشترك.

٥- حل وتسوية الصراعات الدولية

يلعب الفضاء الالكتروني دورا في المساعدة على منع الصراع حيث يمكن أن يستخدم بطريقة سهلة لتبادل الأفكار والتعليم والانفتاح على الأخر، كما إن المعلومات التي يتيحها الانترنت يمكن أن تساهم في تحقيق الاتصال الفعال بين البشر ومن ثم أتاحه الفرصة للتعبيرعن كافة الاتجاهات والتيارات السياسية والقضايا منها ما يتعلق بالقضايا ذات الطابع المحلي أو الدولي، كما يمكن تدويل القضايا المحلية بصورة أكبر.

ويمكن القول إن المساهمة في حل الصراع تختلف عن المصالحة حيث أن حل الصراع يعنى بتلك النقطة التي يستطيع كافة الأطراف في النزاع الاتفاق عليها وتشكل نهاية له، وتستطيع الدول والجماعات المتورطة في الصراع أن تعمل على استقرار السلام من خلال إجراءات يتم من خلالها تطبيق اتفاقيات السلام وتدعيم اطر التعاون وعودة العلاقات الطبيعية ونشر التسامح بين الفريقين، ومن ثم فان حل النزاع يختلف عن المصالحة والتي تعد جزءا إضافيا لإعادة بناء المجتمع ونشر التسامح قبل عملية إعادة بناء الإضرار المادية.

وتظهر أهمية المصالحة التي تتطلب اتخاذ إجراءات عده يكون من شانها أعاده التعمير وإقرار مبدأ العدل والمساواة ومد جسور التعاون، و دوره في تغيير القلوب والعقول ونشر قيم التسامح وبأسلوب متنوع في الرسالة الإعلامية ويستطيع الوصول إلى الأفراد والرأي العام المحلي والدولي حيث يتم توضيح تكلفة الحروب وعوائد السلام ودعم دور المجتمع المدني. وتساعد عملية الانفتاح على مصادر معرفة المتعددة والثقافات المختلفة في دعم من فكرة الاختلاف والتعدد، كما إن توافر المعلومات عن

الصراعات وإعداد الجرحى والقتلى والدمار الذي تسببه من جراء الحروب والصراعات من شأنها أن تساعد على دعم فكرة السلام على حساب فكرة الحرب، كما أن التقدم التكنولوجي والاعتماد الدولي المتزايد عمل على التقليل من نتيجة المعارك الصفرية حيث يصبح جميع المتورطين في الصراعات خاسرين. وهناك العديد من مواقع الانترنت التي تقوم بدور المؤسسات والمنظمات بشكلها التقليدي وفي نفس الوقت عملت على تفعيل المؤسسات المعنية الموجودة من خلال العمل لحل وتسوية الصراعات والحد منها مثل INCORE [1] وهي مبادرة لحل النزاعات العرقية وهو مشروع تابع لجامعه الأمم المتحدة وجامعه الستر بايرلندا الشمالية، حيث يتم توفير قاعدة بيانات عن الدول والصراعات في العالم ويوفر نصوص اتفاقيات السلام.

وأصبحت معظم المواقع الكبرى لمراكز الأبحاث والمواقع المتخصصة في حل الصراعات تتضمن على الأقل قسما خاصا بحل النزاعات، مثل موقع العلاقات الدولية وشبكة الأمن ISN وهو موقع سويسري وانضم بعد ذلك إلى موقع SIPRI [2] لإطلاق مبادرة FIRST[3] الخاصة بالحقائق حول العلاقات الدولية واتجاهات الأمن في العالم، وموقع الأزمات الدولية International Crisis Group [4] ومؤسسة كارنجي للسلام [5] وشبكة البحث عن أرضية مشتركة لحل ومنع الصراعات الدولية[6] وغيرها من المواقع التي تساهم في حل وتسوية الصراعات والنزاعات الدولية. وأطلق معهد السلام الأمريكي مبادرة الدبلوماسية الافتراضية، ويلعب الفضاء الالكتروني دورا في إرساء الدبلوماسية عن طريق التعاون بين مختلف الإدارات الدبلوماسية ودعم الشفافية وتوسيع المشاركة في مجال المعلومات وتبادلها وتحسين قدرات عملية صنع القرار والتفاعل ما بين الرعايا في الخارج وسفاراتهم ونقل وجهات النظر الرسمية إلى الخارج بشفافية، وبما يعمل على تحقيق أهداف السياسة الخارجية للدولة، والمساعدة على القيام بدور في حل النزاعات الدولية عن طريق تقديم اطرعمل ونصوص اتفاقيات دولية وتقديم المشورة حول مناطق النزاع وطرح المبادرات لحلها وحشد الرأي العام الدولي خلفها. و تعزيز من قدرة الدبلوماسي على المتابعة لما يجري داخل بلده أو داخل الدولة التي يتواجد بها، وإتاحة الفرصة للدبلوماسي للتدريب عن بعد عن طريق الانترنت والعمل على رفع قدراته العلمية واللغوية، و تأسيس سفارات افتراضية في المناطق الخالية من الحضور الدبلوماسي أو الضعيفة بتطوير مواقع الكترونية تؤسسها وزارة الخارجية بالدولة المعنية، ذات خدمات موسعة وحية ومتطورة.

(1) للمزيد حول تلك المبادرة يمكن الاطلاع على موقعها على الانترنت على الرابط التالي ،( اخر زيارة ١٢-٧-٢٠٠٧ ) (http://www.incore.ulst.ac.uk/)

(2) يمكن زيارة موقعها والاطلاع على اهدافها وملامح نشاطها على الرابط التالي (اخر زيارة ٢٣-٨-٢٠٠٧ ) ( http://www.sipri.org)

(3) يمكن زيارة موقعها والاطلاع على اهدافها وملامح نشاطها على الرابط التالي (اخر زيارة ٢٣-٨-٢٠٠٧ ) (http://first.sipri.org)

(4) يمكن زيارة موقعها والاطلاع على اهدافها وملامح نشاطها على الرابط التالي (اخر زيارة ٢٣-٨-٢٠٠٧ ) (http://www.crisisgroup.org/home/index.cfm)

(5) يمكن زيارة موقعها والاطلاع على اهدافها وملامح نشاطها على الرابط التالي (اخر زيارة ٢٣-٨-٢٠٠٧ ) (http://www.carnegieendowment.org)

(6) يمكن زيارة موقعها والاطلاع على اهدافها وملامح نشاطها على الرابط التالي (اخر زيارة ٢٣-٨-٢٠٠٧ ) (www.sfcg.o rg/sfcg/sfcg_home.html ).

## المبحث الثالث:

## الفضاء الالكتروني والنظام السياسي الدولي

**يستمر الباحث من خلال هذا المبحث في عرض الاثار الايجابية للفضاء الالكتروني وخاصة فيما يتعلق ببعدة الاقتصادي والسياسي على النظام الدولي، وكيفية تاثير الفضاء الالكتروني على عمل المؤسسات الدولية وبروز فاعليين من غير الدول او مؤسسات من غير الحكومات ، وكيف اثر الفضاء الالكتروني في ظهور نمط جيد من اللبرالية هو الديموقراطية الرقمية وارتباطها بحقوق الانسان الرقمية ، وانماط التاثير على الحراك السياسي الدولي ، وجاء ذلك عبر ثلاثة مطالب الاول يتناول الفضاء الالكتروني والنظام السياسي الدولي والمؤسسات الدولية ، ويتناول المطلب الثاني الفضاء الالكتروني والديموقراطية وحقوق الانسان الرقمية ، واما المطلب الثالث فيتناول انماط تاثير الفضاء الالكتروني على الحراك السياسي الدولي.**

### المطلب الاول:

### الفضاء الالكتروني والنظام السياسي الدولي والمؤسسات الدولية

أصبح الفضاء الإلكتروني مجالاً جديدا للإعلام والصحة والتعليم والتجارة والبنوك والصناعة وحركة المواطن والحكومة الالكترونية، وظهرت الديمقراطية الالكترونية مثل مشاركة المواطنين في استطلاعات الرأي والتعبير عن المعارضة السياسية، و احدث ذلك ثورة في طبيعة العلاقة ونمط الاتصال بين الحاكم والمحكوم وأداء المؤسسات السياسية وفي طبيعة القيم الديمقراطية وبين النخبة والجماهير، ولعب دوراً هاماً في تشكيل كافة التفاعلات السياسية بين السلطة التنفيذية والتشريعية والقضائية والرأي العام والإعلام، وبما يكون له من تأثير على قوة الدولة والاستقرار السياسي.

وإعادة تشكيل القوة والثروة بين أطراف المجتمع وبين غيرها من المجتمعات، وأصبحت شبكة الإنترنت بمثابة الدم لمجتمع المعلومات الذي يمد النظام السياسي بعناصر وجودة وأدوات اتصاله والتعبيرعن تفاعلاته ومخرجاته، خاصة مع ارتباط الإنترنت بالإعلام الجديد أو الالكتروني، و تحقيق التفاعل والتواصل لتحقيق غايات وأهداف معينة قد تكون سياسية أو اقتصادية أو ثقافية، وتكشف العملية السياسية برمتها عن حجم التفاعلات السياسية التي تتم عبر المؤسسات والإجراءات والقيم التي تتحرك داخل النظام السياسي وتشمل المؤسسات الرسمية وغير الرسمية، وأصبحت العلاقة بين تلك المؤسسات بفعل تكنولوجيا الاتصال والمعلومات تتسم بالمرونة وتشابك العلاقات الاتصالية بينها، كما أدت لظهور فاعلين جدداً في النظام السياسي الدولي.[1]

وظهر فاعلون جدد في حركة التفاعل الدولي وظهرت مؤسسات جديدة وسيطة ورأي عام دولي يتحرك عبر مع الانتشار من خلال وسيلة إعلام دولية كالفضاء الإلكتروني، والذي ساعد على زيادة المعرفة والوعي بما يجري في أنحاء العالم المختلفة، و إضفاء نوع من الديناميكية على النظام السياسي الدولي وهو ذلك النظام الذي لا يتقيد بالحكومات الرسمية أو الدول بل إنه يتحرك بالتوافق مع الدول بشكلها الرسمي والمجتمع المدني العالمي والرأي العام الدولي،وذلك مع انتشار القوة السياسية

(1) ماري عوض (مترجم ) ،زكي الجابر ،ثريا متولي(مراجعه واشراف )، ايثيل دوسو لابول (مؤلف )، "التكنولوجيا والسياسة في عصر المعلومات" المنظمة العربية للتربية والثقافة والعلوم ،تونس ،١٩٨٣.

كمجموع الأفعال في المجتمع التي تهدف إلى تنظيمه"[1] وأحدثت تكنولوجيا الاتصال والمعلومات انتشاراً للقوة السياسية داخل المجتمع من قبل فاعلين خارج نطاق النظام السياسي الرسمي ووجود نمط جديد من العلاقة بين المؤسسات داخل النظام السياسي والمؤسسات الخارجية، وأصبحت صناعه القرار السياسي يدخل فيها فاعلون آخرون غير النخبة السياسية أو المؤسسات السياسية المحلية التقليدية، وجاء ذلك مع تعرض الدولة القومية لتآكل سيادتها وفقدان السيطرة على سياستها الإعلامية وقدرتها على تعبئة الرأي العام، وأصبح هناك حالة انفتاح للداخل على الخارج وانتقال مجالات التأثير المتبادل بين دول العالم، كل هذا عمل على التأثير على قوة النظام السياسي ووضعه أمام ضغوط من أصحاب مصالح غير تقليديين، كما إن قوة الدولة المركزية قد ضعفت مع تزايد المطالب المحلية من قبل جماعات عرقية أو دينية بما أدى إلى تقاسم الثروة والسلطة.

وساعد التوجه لتبني تكنولوجيا الاتصال والمعلومات عالميا لزيادة كفاءة الحكومات والقضاء على البيروقراطية، وأصبح هناك تعددية سياسية على مستوى الفكر أو القوى السياسية بدلاً من الأحادية وسيطرة الحزب الواحد. وعمل الفضاء الإلكتروني كمؤسسة سياسية وسيطة وبرلمان مفتوح لكافة التيارات السياسية العالمية، والتأثير على درجة الانتماء الأيدلوجي، و ظهر الاتجاه للتعبئة خلف قضايا عامة محلية أو دولية تهم وتمس المصالح الخاصة بالمجتمع الدولي.

وأثر الفضاء الالكتروني في عمل النظام السياسي سواء ما يتعلق بتوافر المعلومات السياسية أو ما يتعلق بالاتصال السياسي والحشد وتكوين جماعات المصالح والضغط، وذلك بتجاوز المؤسسات السياسية الوسيطة بشكل يظهر نظاماً سياسياً جديداً يرتبط بما يحمله الإعلام الجديد من خصائص وسمات جديدة و بما أثر كذلك على توزيع القوة وظهور فاعلون جدد في العملية السياسية بما اثر على هيكل القوة السياسية والفرص المتاحة للمشاركة في عملية صنع القرار.

وجعل ذلك المؤسسات السياسية تتحرك وتتفاعل إلكترونيا وتغير طبيعة الوظائف التي تقوم بها، ودور المواقع السياسية عبر الإنترنت في تعظيم نقل المعلومات والاتصال الفعال ودورها في فاعلية النظام السياسي وديناميكيته بما يؤثر على طبيعة تطور النظام ودعم الإصلاح السياسي بداخلة.

و أصبح النظام السياسي الجديد مرآه لواقعه المادي وفي نفس الوقت عكس درجة التغير في سماته وخصائصه وطبيعة تفاعلاته وعلاقته بالمؤسسات الوسيطة كالمجتمع المدني والأحزاب السياسية وجماعات المصالح والحركات الاجتماعية والإعلام الجديد وحركات المعارضة، والتي كان لها دورا في الكشف عن الكثير من الممارسات التي تعتبرها هذا الجماعات خاطئة والضغط على السلطات للتحرك باتجاه الاستجابة لمطالبهم، واعتمدت تلك التيارات المعارضة في نجاحها على الفضاء الإلكتروني وقوته الإعلامية الجديدة، والمساعدة في نقل الكثير من الأحداث وكشف التجاوزات من خلال وسائط إعلامية متعددة سواء ما يتعلق بالحكومة أو المجتمع بما يؤثر على الرأي العام بصفة عامة، ومن ثم تصبح وظيفة الحكومة في مراقبة وضبط كل هذه الإمكانيات الهائلة صعبة.

(1) Jan A.G.M. van Dijk, **Models Of Democracy And Concepts Of Communication, Digital Democracy**, Issues Of Theory And Practice, Sage Publications Copyright, (2000),pp 1-23.

ويظهر تأثير الفضاء الالكتروني على هيكل النظام السياسي الدولي في توفير أدوات للتأثير على الرأي العام وما يتم توفيره من معلومات تدفع النظام السياسي للتغيير بما يتوافق مع هذه الضغوط بالإضافة للتأثير على القيم المحلية التي تشكل وجهة النظر تجاه النظام السياسي، وعملية صنع القرار والتفاعلات بين المنظمات المختلفة وجماعات الضغط في مواجهه الرأي العام، وذلك في اطار تأثير الشبكات المعلومات العالمية على القيم المحلية والثقافية [1] وهيكل النظم السياسية بما يظهر في قلب تفاعلاتها ، ودعم قدره المنظمات على التفاعل بدرجة عالية مع المنظمات الأخرى في نظام سياسي تعددي، وهذا ما يمثل في الوقت نفسه ممارسة ضغط غير مباشر على هذه المنظمات لإصلاح هياكلها الداخلية و المؤسسية من اجل دعم قدرتها على الاستجابة والفاعلية في مواجهه المطالب والضغوط.

و أدت التطورات التكنولوجية إلى لامركزية السياسة وانتشارها داخل المجتمع الدولي ،وانتقالها من الدور المركزي للدول القومية بمؤسساتها السيادية إلى فاعلين آخرين من غير الدول مثل المنظمات الدولية والشركات الدولية متعددة الجنسيات والمجتمع المدني العالمي والجماعات والأفراد، وتصاعد دور المجتمع المحلي في أولا صنع السياسة المحلية ثم التأثيرعلى طابعها الدولي، والقدرة على التواصل مع الخارج ثقافيا وسياسيا واجتماعيا دون المرور بالضرورة بمؤسسات الدولة الرسمية والقدرة على تنوع وسائل الإعلام ومصادر المعلومات بعيدا عن احتكار الدولة التقليدي لها.

واصبح النظام السياسي متعدد المراكز والأطراف والفاعلين عبر شبكة تفاعلية متصلة عن طريق تكنولوجيا الاتصال والمعلومات، وظهر الدور القوي للمؤسسات المالية الدولية والشركات متعددة الجنسيات وجماعات المصالح والمنظمات الدولية ،والتي أصبحت تستخدم تكنولوجيا الاتصال والمعلومات في جمع المعلومات وممارسة المزيد من الضغط على الحكومات بالإضافة للمساعدة في نمو المجتمعات المحلية وانتشار الطابع اللامركزي للإدارة. جاء ظهور المجال العام الالكتروني كأحد التأثيرات الهامة على النظام السياسي، وخاصة تلك المنظمات الوسيطة ودورها بعد أن أدت الثورة التكنولوجية إلى تآكله والتأثير فيه، وظهرت ديمقراطية جديدة ذات طابع الكتروني بما أثر على العملية السياسية برمتها، [2]

ويمثل أساس عمل المؤسسات الوسيطة الدولية في توفير الرابط السياسي بين المواطن والحكومة داخل الدولة وعلى المستوى الدولي، وهذا الرابط السياسي من شانه إن يجعل هناك اتصالاً بين عنصرين، ويعد هذا الرابط آلية يمكن من خلالها السماح للقادة للتصرف بما يتواكب مع الحاجات والمطالب والرغبات الخاصة بالجمهور. و أثر الفضاء الإلكتروني في المنظمات الدولية حيث ساعد على جمع المطالب السياسية والقضايا الدولية، والعمل على توفير المعلومات التي تساعد في عملية صنع

(1) Christophe Engel Kenneth H.Keller (eds.):**Understanding the Impact of Global Networks on Local Social,** Political and Cultural Values", Lorenz Muller," Global Networks and Local Values" , **Law and Economics of International Telecommunications** [42]),Baden-Baden (Nomos) 2000 ,pp 284-316.

(2) A.M. Chircu and R.J. Kauffman, **Strategies for Internet middlemen in the intermediation/disintermediation/reintermediation cycle,** Electronic Markets 9(1/2) (1999), 109–117.

القرار، وتسهيل عملية التفاعل حيث تتكون عمليات صنع القرار في الشبكات التي تزيد عن أهمية الأدوار التفاعلية للمؤسسات الوسيطة ويكون له تأثير على عمليات التفاوض والوساطة.

وأصبحت وسائل الإعلام الالكتروني الجديد لها دور في تشكيل أنماط معينة من السلوك الإنساني وتهميش أنماط أخرى من خلال لغة الصورة ورموزها. إذ بموجب ذلك أدركت الدول المتقدمة أهمية الأدوار التي يمكن أن يقوم بها الإعلام كبديل لممارسة الديمقراطية خصوصاً بعد أن احتلت وسائط الاتصال المساحة المخصصة لممارسة الفعل الديمقراطي، وأصبحت هذه المساحة هي ذاتها المخصصة للإعلام، ولذلك لم يعد الإعلام يمثل السلطة الرابعة، بل أصبح يشغل المجال بين الفعل السياسي والثقافي في ورد الفعل الجماهيري في كافه أرجاء العالم، وقدمت تكنولوجيا الاتصال والمعلومات نفسها تدريجيا كآليات وكمحاولة في ذات الوقت لتقوية وظائف المنظمات الوسيطة أو لأعاده تنشيط دورها على الأقل في الحياة العامة كإدخال آلية التصويت الالكتروني في البرلمان أو توفير معلومات متسارعة للنواب بما يؤثر على أدائهم أو دعم حملاتهم الانتخابية .

وشجع الفضاء الإلكتروني في ظهور مؤسسات وسيطة جديدة ومتعددة عبر مواقع الإنترنت حيث انخفاض تكلفة انشاء الموقع وسهولة الانتشار وزيادة الفاعلية وذلك الى جانب انها عمل في ذات الوقت على تنشيط ما هو قائم من منظمات دولية حكومية او غير حكومية بالاضافة الى المجتمع المدني ، والقدرة على تعبئة الرأي العام الدولي خلف قضايا محددة، حيث تكون المجتمعات التي تتمتع بشبكات حديثة تكون عملية صنع القرار فيها منتشرة أو ترتبط بمستويات أفقية جماهيرية، ومستويات عدة من الحكومة واتساع حجم ودور الفاعلين في العملية السياسية أو المنظمات والمجتمع المدني والشركات الخاصة. وأدي ذلك إلى ظهور شكل جديد من الحكم يشارك فيه فاعلون كثر من أجل تحقيق غاية أو هدف معين، والذي يتم تحقيقه بالتوافق بين الأهداف المختلفة للمواطنين ليتم صياغتها للتأثير على صانعي القرار، وظهور هذه الأشكال الجديدة من الحكم بما يمكن ان تسمى بمرحلة التحول إلى "الدولة ما بعد البرلمان "[(1)]

وأصبح هناك سهولة في عملية الانتقال والإرسال ما بين أفعال الحكم وردود أفعالة ومصالح المواطنين مع وجود إلية خاصة لتحقيق ردود الأفعال والاستجابات بين الطرفين[(2)] وهناك ممارسة مختلفة للسياسة عن طريق دور تكنولوجيا الاتصال والمعلومات في دفع العلاقة والتفاعل البناء ما بين المواطنين وأجهزة الحكم، وأصبحت المجتمعات أكثر شبكية كلما كانت أكثر التصاقا بقضايا المواطنين وتعبيرا عن مصالحهم، وذلك بالاختلاف مع الممارسة السياسية التقليدية التي كانت تعتمد على المؤسسات الوسيطة فقط. ويتم استخدام تكنولوجيا الاتصال والمعلومات لتسهيل إيجاد أشكال جديدة من التمثيل والعمل السياسي والمحاسبة، وذلك لأنها تجعل هناك فرصاً لإيجاد أنواع جديدة من

(1) S. Coleman, J. Taylor and W. van de Donk, (eds), **Parliament in the Age of the Internet**, Oxford University Press, Oxford,1999.

(2) Ph. E. Agre, **Real-Time Politics: The Internet and the political process**, The Information Society 18 (2002), pp 311–331.

المؤسسات الوسيطة في العملية الديمقراطية وذلك بعيدا عن أشكالها التقليدية.[1] وتوفر الخيارات المتعددة لتمثيل المصالح والتعبيرعن المشاكل،و جذب الجمهوروالمهتمين بالشأن العام أو فيما يعرف بالمواطن العالمي، الذي يتحرك ويتفاعل مع القضايا العالمية مع اتساع وتمدد جمهور المستخدمين و القدرة على بناء قنوات اتصال متعددة[2] وقام الفضاء الالكتروني عبر مواقع الإنترنت ووسائل الاتصال والمعلومات من خلال ما تتيحه من نقاش عام حول القضايا السياسي بفتح مجال عام مفتوح للحوار داخل البيئة السياسية والتنظيمية، والقيام ليس فقط بدور المؤسسات السياسية الوسيطة بل أيضا القيام بملء الفراغ الذي يوجد نتيجة عدم وجود مثل تلك المؤسسات أصلاً داخل المجتمعات المحافظة التقليدية.

## المطلب الثاني:

## الفضاء الالكتروني و الديمقراطية و حقوق الانسان الرقمية

يتميز الفضاء الإلكتروني بخصائص أهمها حرية الاستفادة من المعلومات الشخصية والحصول عليها وحرية إنتاجها وتعدد مستويات الخدمة، و لا يوجد مظاهر تمييزية، وارتفاع سقف الحرية في التعبير والمشاركة، و رخص التكلفة بما يجعله في متناول الجميع، و يمكن لأي فرد أن يستفيد من الخدمة دون تمييز بسبب الدين أو اللون أو العرق أو الجنس، وإتاحة الفرصة للكافة في المشاركة في الرأي أو إضافة المحتوى أو التعليق دون قيود، و تنوع وسائل الرسالة الإعلامية من الصوت والصورة إلى الفيديو والنص.

وظهر الدور الإيجابي لتكنولوجيا الاتصال والمعلومات في إشاعة المناخ الديمقراطي، فيما يتعلق بتغيير أدوات وآليات الممارسة الديمقراطية، وتوفير البنية التحتية لإنتاج وتداول المعلومات عن طريق شبكات الاتصال، والعمل على استغلال وترتيب وتخزين هذه المعلومات، وساعدت تكنولوجيا الاتصال والمعلومات على تعدد صور تداول تلك المعلومات سواء أكانت بالكلمة والصوت والصورة، وفتحت تكنولوجيا الاتصال والمعلومات مجال لتجميع واستغلال وتوزيع لـ"الثقافة"، بشكل رقمي تكون فيها الشبكات أدوات للترويج لها. وأنتج ذلك ظاهرة ذات بعدين احدهما يحمل بعدا سياسيا، أما الأخر فهو بعد تكنولوجي وأخذت العلاقة بين هذين البعدين تتزايد و تفرض نفسها على الواقع السياسي والاجتماعي والاقتصادي الدولي. وظهر التزاوج والتلاحم ما بين أدوات ممارسة المواطن لحقوقه السياسية والديمقراطية من ناحية وبين منجزات ثورة تكنولوجيا المعلومات والاتصالات من ناحية أخرى[3] ومثلت شبكة الإنترنت أهم بنية تحتية لمجتمع الإعلام المتنامي من جميع البلدان والثقافات واللغات والفئات العمرية المختلفة والمهن دون تمييز. وبدأ هذا الدور في الظهور منذ منتصف التسعينات في دعم مفهوم وممارسة الديمقراطية، وأخذ هذا الدور في التبلور المتصاعد مع النمو المتزايد

(1) U. Josefsson and A. Ranerup, **Consumerism revisited: the emergent roles of new electronic intermediaries between citizens and the public sector,** Information Polity 8 (2003), 167–180.
(2) K.L. Hacker and J. van Dijk, **What is digital democracy?, in: Digital Democracy. Issues of Theory and Practice,** K.L.Hacker and J. van Dijk, eds, Sage Publications, London, 2000, pp. 1–10.
(3) C. Bryan, R. Tsagarousianou and D. Tambini, **Electronic Democracy and the Civic Networking Movement in Context,** in: Cyber democracy: Technology, Cities and Civic Networks, R. Tsagarousinou, D. Tambini and C. Bryan, eds, Routledge,London and New York, pp. 1–17.

في انتشار تكنولوجيا الاتصال والمعلومات، والذي ظهر في إعادة تنشيط المجال المدني وتوسيع نطاق الحياة المدنية وفتح مجالات واسعة عن طريق تنوعه وسرعته وتحديه للحدود الجغرافية، وإتاحة الفرصة امام العديد من البشر المختلفون في توفير فرص للتفاعل والاتصال فيما بينهم حول الجدل السياسي العام وعملية صناعه القرار، وأداة في التعبئة والتجنيد والتنظيم والتصويت والمعارضة.

وأتاح الفضاء الالكتروني من خلال عملية استطلاعات الرأي والمشاركة في الانتخابات للعديد من الناس أن يعبروا عن أرائهم بشكل منتظم و اتساع دورهم في عملية صنع القرار، و سد الفجوة بين المواطنين ومن يمثلونهم في المجالس النيابية. ونشوء أشكال جديدة من وسائل الإعلام مترافقة مع نماذج جديدة لتوزيع المعلومات واستهلاكها واستخدامها، و تم تخطي الخطوط التقليدية الفاصلة بين الجمهور والمؤسسات الإعلامية مع اكتساب المواطنين إمكانية الوصول إلى منابر جديدة يمكنهم من خلالها التعبير عن آرائهم وأفكارهم الخاصة، ويتجاوزن بذلك المؤسسات الإعلامية الكبرى والحكومات التي ظلت لمدى طويل صاحبة القرار النهائي بتحديد المعلومات التي يتم نشرها [١].

وعلى الجانب الأخر الفضاء الالكتروني على نمو الهويات المحلية والولاءات التقليدية الضيقة بداخل المجتمعات القومية ، وزيادة حجم التعبئة الطائفية على أسس سياسية واجتماعية والمساعدة في بث الكراهية الدينية ،واصبح للفضاء الالكتروني دور في إحداث تغييرات في بنية المجتمع الثقافية والاجتماعية والسياسية ، و دور فاعل ومؤثر في عملية إنتاج وإدارة وتوزيع العملية الثقافية في العالم والقدرعلى إتاحة الفرصة للتعرف على ملامح مختلفة للثقافات العالمية [٢] . وأثر الفضاء الالكتروني على درجة التماثل الثقافي الذي كانت تتمتع به المجتمعات القومية حيث ظهرت قوى ومجموعات جديدة تستطيع التعبيرعن ثقافتها وقيمها المختلفة بعيدا عن السياق العام لها ، وأصبح يحاكي البيئة الاجتماعية الطبيعية من جراء وجود مجتمعات افتراضية، وتجمهرات رقمية على شبكة الإنترنت والتفاعل بين مختلف أنواع البشر لهذه الجماعات الالكترونية [٣]

وأوجد التزاوج بين السياسة والتكنولوجيا بصفة عامه تأثيرا شاملا على العملية السياسية والنظام السياسي بشكل دعي إلى ظهور ما يمكن إن يطلق علية" النظام السياسي الالكتروني أو الافتراضي " والذي ظهر مع انتقال مجالات الصحة والتعليم والتجارة والحكومة وحركة المواطن والاستجابات حول صناعه القرار الحكومي إلى الفضاء الإلكتروني وظهور أساليب جديدة للتعبير عن الرأي. واصبح للفضاء الالكتروني دور في تفاعلات العملية السياسية وكذلك على التنمية الاقتصادية، وتعزيز عملية التحول الديمقراطي ومواجهة الممارسات الاستبدادية، وما يكون ذلك من أثر عميق وممتد في احداث التحول والحراك السياسي في النظام الدولي. وتأثرت الدول النامية بدرجة اكبر من الدول المتقدمة ديمقراطيا حيث مثل الفضاء الالكتروني من اكثر الوسائل حرية وانفتاحا عن وسائل الاعلام التلقدية

(1) موقع وزارة الخارجية الامريكية http://usinfo.state.gov/journals/itgic/0306/ijga/welcome.htm

(2) عادل عبد الصادق ،" حقيقة دور الانترنت في بث الكراهية الدينية في العالم " ، ملف الاهرام الاستراتيجي ، مركز الدراسات السياسية والاستراتيجية بالاهرام ، العدد١٤٤ ، ديسمبر ٢٠٠٦ .

(3) د.علي محمد رحومة، " علم الاجتماع الآلي،" سلسلة عالم المعرفة ، المجلس الوطني للثقافة والفنون والآداب، الكويت ٢٠٠٨، ص ص ٥٦-٧٨ .

التي تخضعها لسيطرة الدولة، أما الدول المتقدمة فلديها العديد من وسائل الاتصال وعلى درجة كافية من الحرية، وأصبحت التكنولوجيا ليس فقط أداة اتصال وتواصل بل ووسيلة حقيقية للتعبير وحرية الاتصال والحق في الإعلام، وأداة من أدوات تكريس إن لم تكن الديمقراطية المكتملة فعلى الأقل دعم قيم المواطنة باعتبارها مكمن واجبات الأفراد والضامن الأسمى لحقوقهم.، ولا تعبر فقط الديمقراطية الالكترونية عن مجرد أنها تحمل طابعا فنيا أو تقنيا، بل أنها ترتبط بالبيئة السياسية والاقتصادية والاجتماعية والثقافية. وأصبحت الشبكات الإلكترونية وسيلة لدفع العازفين عن المشاركة في العمل السياسي للمساهمة في تحديد حال ومآل الشأن العام بدلا من اللجوء إلى وسائل الإعلام التقليدية أو تعدي معوقات المشاركة السياسية [1]

ودفع تزايد انخراط الثورة الالكترونية في نسيج الحياة اليومية لزيادة تعمق التشابك بين التطورات التقنية من جهة والبني الاجتماعية والسياسية والثقافية من جهه اخرى ظهورنمط جديد من الحقوق أصبحت تدافع عنه منظمات خاصة بالدفاع عن حقوق الإنسان، واعتبرت الحرية الإلكترونية Electronic Freedom جزءاً من المسار الديمقراطي عالمياً ،وفي السياق نفسه، نشأت منظمات تتخصص في ملاحظة هذا البُعد الجديد في الممارسة الديمقراطية، على مستوى الأفراد والشعوب، مثل"منظمة الدفاع عن الحقوق الالكترونية المواطن" الأمريكي ومبادرة الحقوق الرقمية [2]وذلك كجزءمن اهتمام منظمات حقوق الإنسان، والتي استفادت من تلك الآليات التكنولوجية كالإنترنت والاتصالات المتطورة في القدرة على الدفاع عن حقوق الإنسان وتعميق النقاشات الديمقراطية عالمياً [3] .

وأصبح الفضاء الإلكتروني مجالاً للنشر والصحافة الالكترونية وتعبيرعن ظهور حقوق إنسان ذات طابع رقمي فيما يطلق علية "بحقوق الإنسان الالكترونية" والتي ما هي إلا امتداد لمثيلتها المادية و شهد المجتمع الدولي في العقد الأخير مظاهر ثورة إعلامية جديدة من أهم مظاهرها سهولة الحصول على المعلومات، وانتشارها ، والقدرة العالية على صياغة الرسالة الإعلامية حسب ما يريدها القائم بعملية الاتصال دون تدخل موجة من الرقابة التقليدية للدولة أو الأقطاب الإعلامية الكبرى المحتكرة للوسط الإعلامي. وتميزت الثورة الإعلامية الجديدة في مظاهرها برخص ثمن الاتصالات مما يجعلها متاحة للجميع، ولا مجال لاحتكارها من طرف الحكومات أو الشركات الاحتكارية [4] وتشكل السوق المفتوحة للأفكار بيئة عمل للتكنولوجيا و الإبداع والابتكار كوسيلة للاستمرار ويعزز من الطابع الإنساني والقيم الإنسانية المشتركة.، بالإضافة إلى حماية خصوصية الأفراد و الحق في المعرفة وحق المواطن في الإعلام و صنع القرار وغيرها من الحقوق التي أصبحت لصيقة الصلة بتكنولوجيا الاتصال والمعلومات والتي تعمل على تقوية التنظيم السياسي والشرعية السياسية ،وبما يظهر في شكل إحداث تغيير سياسي تدريجي أو جذري .

(1) يحيي اليحياوي،" التكنولوجيا والإعلام والديمقراطية"، دار الطليعة للطباعة والنشر، بيروت ، الطبعة الأولى، ٢٠٠٤، ص ص ٢٣-٧٨.

(2) موقعها على شبكة الانترنت( http://www.dfi.gov)

(3) جريدة الحياة ، ١٤-١-٢٠٠٧

(4) محمد المختار الشنقيطي،" الإعلام والسياسة في عصر الإنترنت"،مجلة العصر ، ٢٢-٩-٢٠٠٢
(http://www.alasr.ws/index.cfm?method=home.con&contentID=3033)

## المطلب الثالث:

## انماط تاثير الفضاء الالكتروني على الحراك السياسي الدولي:

١- الفضاء الالكتروني والتنمية السياسية وتضييق فجوة المعرفة السياسية

ظهر مجتمع المعلومات الذي يتميز بتصميم وإنشاء وتقييم واستخدام وصيانة منظومات معالجة المعلومات بما تشتمل عليه من معدات Hardware وبرمجيات Software وجوانب تنظيمية، وموارد بشرية هذا بالإضافة إلى مجموع الآثار الصناعية والتجارية والإدارية والسياسية والاجتماعية المترتبة على تلك المنظومات، وفي مجتمع المعلومات يمكن التمييز بين أنواع مختلفة من المعرفة، والتي تكون أوسع من مفهوم المعلومات، حيث تتكون من معرفة ما Know What تشير إلى معرفه عن الحقائق السياسية التي يمكن أن تتحول إلى معرفة رقمية في شكل معلومات وبيانات تتحول إلى موقف سياسي ثم اتجاه يتم ترويجه للرأي العام، ومعرفة كيف Know how تشير إلى المهارة و القدرة على فعل شيء ما عن طريق تدريب الكوادر السياسية التي تتعامل مع المعلومات السياسية وكيفية إدارتها ومعرفة لماذا Know why، تشير إلى المعرفة العلمية لمبادئ وأسس التنمية السياسية والتي تشكل الدفع للتنمية في الأحزاب السياسية أو المنظمات الوسيطة، ومعرفة من know who وتتعلق بمن يستطيع إن يملك القدرة والمهارة السياسية لحشد الرأي العام ولدية من الخبرات التنظيمية والسياسية والإعلامية التي تؤهله للتأثير، بما يساعد على عملية الحراك السياسي داخل النظام السياسي والنخبة السياسية.

ويمكن القول أن التعليم لهذه الأنواع الأربعة الرئيسية للمعرفة السياسية تحدث من خلال القنوات المختلفة، وهناك نوعان من المعرفة يمكن الحصول عليهما من خلال قراءة الكتب أو حضور المحاضرات وإدخال البيانات، إما النوعان الآخران من المعرفة فيرتبطان بشكل أساسي بالممارسة العملية.[1]

ويحرك النمو السريع في انتشار تكنولوجيا الاتصال والمعلومات هو توق المواطن للحصول على المعلومات والإطلاع على كل ما يخص حياته وأخباره المحلية بدون إن يكون للرقابة الحكومية أي دور في تحديد ماهية تلك المعلومات والإخبار المنشورة، وأصبحت العملية السياسية بتفاعلاتها وأطرافها ومؤسساتها تشهد تأثيراً ايجابياً على تقليل حجم النفقات في العديد من الأنشطة السياسية اللازمة للمجال السياسي العام، وساهمت في زيادة الكفاءة الإدارية خاصة تمكن الأطراف السياسية من إدارة سلاسل العرض والطلب بطريقة أكثر فعالية، وزيادة التنافسية بين فاعلي العملية السياسية، وعملت على جعل رأس المال السياسي أكثر شفافية. وعمل الإنترنت على تضييق فجوة المعرفة السياسية و حرية تداول المعلومات وانتشارها وحرية الوصول إليها وقدرة أي فرد على المساهمة فيها وإنتاجها و إزالة اللبس والغموض المعرفي سواء ما يتعلق بالقضايا الداخلية أو الخارجية بجمع المعلومات و التعليق عليها والتحاور حولها، ثم اتخاذ خطوات فعلية.

[1] **Towards: knowledge societies** , unesco world report ,UNESCO, 2005,pp 200-340 also available at (http/www.uesco.org/publications)

٢- الفضاء الالكتروني و بناء رأس المال الاجتماعي للديمقراطية المحلية

أدت ثورة الإنترنت إلى تنشيط المجتمعات المحلية وزيادة الروابط بين الأفراد والمجتمع حيث زيادة الحالة التفاعلية بين الأفراد سواء أكان في شكل فردي أو في شكل تنظيمات سياسية وحركات اجتماعية تدعو إلى الحكم الديمقراطي، والعمل على بناء هويات محلية فاعلة تسعى لأن يكون لها دور في اللعبة السياسية ، وتساهم بوابات الإنترنت في تقديم الخدمات الحكومية العامة بما يعمل على التواصل المحلي مع المواطنين دون وسطاء حكوميين، وإلى الوصول لدرجة عالية من الرضاء عن أداء الحكومة والقدرة على تقييمها .

وبما يساعد على الارتباط القوى مع المجتمعات المحلية وتشجيع دورها في صنع القرار بالإضافة إلى دور المجتمع المدني والحكومة اللامركزية، و إعادة تشكيل القوة والثروة بين أطراف المجتمع على المستوى الداخلي او بين غيره من المجتمعات ، وبما يعمل على تعظيم رأس المال الاجتماعي من خلال نوعان من رأس المال الاجتماعي الأول: يتم عن طريق دعم التواصل والتفاعل بين الناس المتشابهين مع بعضهم البعض، أما الثاني فهو يتعلق بمد الجسور والاتصال بالناس الذين يختلفون عن غيرهم، ومن ثم فان الفضاء الالكتروني كأداة اتصال ووسيط في التمية البشرية حيث يعمل على رفع القدرات على مستوى التعليم والتدريب ،وبما يساهم في تسريع تراكم رأس المال الاجتماعي.

٣- الأحزاب السياسية بين القوة والضعف

عملت تكنولوجيا الاتصال والمعلومات على تقويةعمل الأحزاب السياسية بما أتاحته من فرص وقدرة على إنشاء مواقع حزبية على الإنترنت والتفاعل مع الزائرين، وما يتضمن من نشر الإخبار والخلفية التاريخية للحزب السياسي وبرنامجه الانتخابي، وانشاء قناة اتصال بين قاده الحزب والقاعدة الجماهيرية عن طريق البريد الالكتروني أو برامج الدردشة أو الاستفتاءات حول أداء الحزب في الانتخابات والتي من شأنها المساعدة في ترشيد القرار السياسي للحزب السياسي، وتفعيل علاقته بالرأي العام عن طريق تطوير إستراتيجيته الانتخابية، ويستطيع الحزب السياسي عبر موقعة على الإنترنت الحصول على أعضاء جدد وحشد وتعبئة أعضائه وتنسيق الفعاليات السياسية الخاصة به، واجتذاب الأجيال الجديدة الشابة من خلال إضفاء المزيد من الجاذبية والتنوع على مواقعها على الشبكة، وفي الدعاية والإعلان عن نشاطها والحصول على التمويل والتبرعات لنشاطها والتجنيد والحشد والتعبئة لمؤيدها وتحقيق عملية الترابط بينهم، وتبادل المعلومات والتخطيط والتنسيق.

ودفع الإنترنت للتأثير الإيجابي على دور الأحزاب السياسية عبر التصاقها الجديد بالجماهير، ونشر برامجها وانتفاء العلاقات الهرمية داخل المؤسسة الحزبية. ويمكن أن تستفيد الأحزاب السياسية من خلال ثلاث وظائف للانترنت هي التشارك في المعلومات وتقديم الخدمات والدخول كقوة سياسية في عملية صنع القرار، وعلى الرغم من دور تكنولوجيا الاتصال والمعلومات في توفير فرص لنهوض العمل السياسي دخل الأحزاب إلا أنها قد مثلت أداة كاشفة لمواطن ضعفها وانعزالها عن المحيط الاجتماعي الذي تعمل من خلالة، وكشفت عن مشكلات تنظيمية وحتى فكرية داخل بنيتها الحزبية، والدفع بفاعلين جدد تجاوزا لدور تلك الأحزاب كمؤسسات وسيطة.

٤- الفضاء الالكتروني وخلق بيئة إعلامية جديدة بديلة لوسائل الإعلام التقليدية

أصبح الفضاء الإلكتروني اقرب إلى برلمان عالمي يستطيع كل فرد إن يعبر عن رأيه وفكرة ويشارك في صنع القرارات ، وتم تشكيل مجموعات افتراضية شبيهة بالأحزاب السياسية، وتساهم كجماعه ضغط الكتروني تؤثر على القرارات السياسية للحكومات وتؤثر في عملية صنع قرارات السياسة العامة، وأصبح هناك تواصل وتفاعل مباشرة بين القادة والمحكومين والرؤساء عبر الاتصال المباشر عن طريق مواقع الإنترنت، والتي تنقل حركة التفاعلات السياسية السلمية أو الصراعية بما يساعد في عملية صنع القرار في دوائر السياسة الخارجية في العديد من دول العالم، وخاصة مع ظهور الفضاء الالكتروني كمنافس لوسائل الإعلام التقليدية، وبقدرته على تخطي الحدود التقليدية .

وأصبح مشجعا للتحول السياسي بداخل النظم الاستبدادية، ودورة في التنشئة ونشر الثقافة السياسية بما يؤثر على الحراك السياسي والاجتماعي، وأدي لتطوير أساليب العمل الاجتماعي في إطار تحول الإنترنت لوسيلة إعلام دولية مع اندماج كل من أنواع الإعلام التقليدية مثل الإعلام المقروء والمسموع والمرئي داخل الإنترنت، والذي عمل على إتاحة المعلومات بحرية وتبادلها وانتشارها بسرعة ونقل وجهات نظر مختلفة عما تروجه وسائل الإعلام الرسمية والصحف التقليدية عن طريق الصحافة للجمهور.[1]

وشكلت أدوات الرأي والتعبير عبر الإنترنت أحد روافد الإعلام الالكتروني من خلال قدرة الفرد اتخاذ المبادرة وصياغة المادة الإعلامية وتشكيلها والعمل على انتشارها، مع الحرية في اختيار الموضوع وتحرير النص والحجم وتوقيت النشر وسهولة البث وقلة التكلفة، بالإضافة إلى إمكانية تجاهل المصدر. ويكون متاح لمستخدمي الإنترنت استخدام كافة الوسائل التقنية في إخراج رسالة إعلامية تجمع بين الصوت والصورة والكتابة والخلفية الموسيقية بشكل يجذب إليها الجمهور. وكان لذلك تأثير على المؤسسات الإعلامية الرسمية والتقليدية سواء في طبيعة دورها أو نشاطها وقدرتها على التأثير في الرأي العام.

وأدى الإعلام الالكتروني إلى الانتقال من الإعلام الجماهيري إلى إعلام فردي يمكن أن يوجهه الفرد للتأثير على الرأي العام وعلى السياسات الحكومية بعيد عن المؤسسات الوسيطة. وشكل بدورة الإعلام الالكتروني بيئة جديدة تستطيع كافة التيارات الفكرية والسياسية والثقافية والدينية التعبير عن نفسها بحرية وبدون أي حواجز أمنية أو جغرافية، وأداة لنقل معاناة المهمشين في حياتهم ومشاكلهم اليومية، وذلك بعيدا عن هرمية المؤسسات التقليدية بشكل أثر على فاعلية المعلومات المتاحة بما يخدم التمثيل السياسي للمواطنين وعلى دور الأحزاب السياسية والمجتمع المدني .

وظهر الإعلام الالكتروني كبديل عن المؤسسات التقليدية والصحف الورقية، وبشكل عمل على جذب الأفراد للتعبير عن أرائهم بشكل مختلف عن الرقابة الرسمية وبرؤية مغايرة عما تداوله الصحف الرسمية الورقية، وتميزه بسهولة الحصول على المعلومات وانتشارها وانخفاض تكلفتها وصياغة الرسالة

[1] عادل عبد الصادق "الانترنت والاصلاح السياسي في مصر " مجلة تعلقيات مصرية، مركز الدراسات السياسية والاستراتيجية بالاهرام، العدد، ٨٣ ،١٥ يوليو ٢٠٠٧ يمكن الاطلاع علية على الرابط التالي ( اخر زيارة ٣٠-١٠-٢٠٠٨ ) (http://acpss.ahram.org.eg/Ahram/2007/7/15/COMM0.HTM)

الإعلامية بشكل جيد، وبما أدى لكسر احتكار الدولة لوسائل الإعلام الجماهيري وتوسيع قاعدة المساهمين في تشكيل قضايا الرأي العام بدلا من دور النخبة التقليدي، وشكل ذلك ضغطا على الحكومة تجاه ترشيد سياستها العامة، كما ساعد الإنترنت على تحسين دور وأداء الصحافة التقليدية على المتابعة الجيدة وتعزيز مهنيتها بالإضافة إلى الحد من دور الصحافة الحزبية والأيدلوجية.[1]

٥- الفضاء الالكتروني وتحسين ظروف إدارة العملية الانتخابية

أصبح للفضاء الالكتروني دور في تحسين جودة العملية الانتخابية و إدارتها وما يتعلق بالحملات الانتخابية وإعمال الدعاية والتواصل مع الناخبين، ثم نظم التصويت وتجميع وفرز وعد الأصوات وإعلان النتائج ثم آلية استطلاعات الرأي واليه الاستفتاءات السريعة علي القرارات وآليات حرية التعبير عن الرأي، بحيث يقوم الحكام والمواطنون علي السواء باستخدام هذه الأدوات الكترونيا ورقميا إما بشكل جزئي أو كلي.، أو ما يتعلق بعملية التصويت دولية النطاق كمثل تلك التصويت إلى أجريت لاختيار عجائب سبع جديدة أو مواقع التوقيعات الالكترونية للمطالبة أو تأييد موقف ما ويتيح التصويت الالكتروني في الانتخابات للناخب التصويت بسرية وبأمان وبدون تدخل أي من السلطة التنفيذية إلى أن تطول عملية عد الأصوات وفرزها آليا ولتعلن النتائج الكترونيا دون تدخل أي من فرقاء العملية السياسية.

وأصبح لتكنولوجيا الاتصال والمعلومات دورا في التأثير على العملية الانتخابية في أدوات تنفيذها وسير إجراءاتها، بل وفي القيم التي تحرك المشاركة السياسية بما يتم بثه عبر أدواتها وفي الحملات الانتخابية وأعمال الدعاية والتواصل مع الناخبين، واتاحة الفرصة لذوي الاحتياجات الخاصة وكبار السن والنساء للتصويت من بيوتهم عبر الإنترنت، وبما يساعد على زيادة المشاركة السياسية، فضلا عن سهولة نظام التصويت الالكتروني ودقته في عملية التصويت وفرز وعد الأصوات وإعلان النتائج وذلك على نحو أثر في معادلات ومعالجة ونتائج العملية السياسية برمتها.

ويشكل عظم من حيادية إدارة العملية الانتخابية ويضاف إلى ذلك قلة تكلفتها، وتميزها بالنزاهة والشفافية بما يساعد على حفز المشاركة السياسية ووصول الناخب للمعلومات بأسلوب سهل وجذاب عبر طرق يمكن الوثوق بها وأثر ذلك في إلغاء العديد من الوسطاء في العملية الانتخابية بما يحد من الفساد السياسي والانتخابي وتحسين جودة العملية الانتخابية سواء في مرحلة الترشيح أو التصويت أو النتائج، وذلك من خلال ما أتاحته تلك الوسائل الجديدة كالإنترنت والكمبيوتر والهواتف المحمولة من دور في عملية الدعاية للمرشحين والتعريف بالمرشح، وإعداد قوائم انتخابية لا يشوبها الأخطاء الإملائية أو التزوير عن طريق استخدام البرامج الإحصائية الالكترونية وجود قاعدة بيانات وسجلات انتخابية الكترونية . ويكون لذلك تأثير إيجابي على تقليل حجم النفقات في العديد من الأنشطة السياسية اللازمة للمجال السياسي العام، كما ساهمت في زيادة الكفاءة الإدارية، وخاصة تمكن الأطراف السياسية من إدارة سلاسل العرض والطلب بطريقة أكثر فعالية، وزيادة التنافسية بين فاعلي العملية

(1) عادل عبد الصادق، " المدونات كفاعل ونمط جديد للمشاركة السياسية "، ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالاهرام، العدد ١٥٠، يونيو ٢٠٠٧.

السياسية و جعل رأس المال السياسي أكثر شفافية ،وعن طريق الإنترنت والهاتف المحمول والاتصالات يتمكن المرشح السياسي من أن يتواصل مع جماهير الشعب مباشرة دون الحاجة إلى طرف ثالث ليكون بمفردة من يحرك دفة الحوار، والمساعدة في الدعاية الانتخابية عن طريق إنشاء مواقع للمرشحين عبر الإنترنت وبث حملتهم الدعائية لجذب التبرعات والمؤيدين. وجمع التمويل والتبرعات للحملات الانتخابية، وتعدد البدائل السياسية أمام المواطن أو الناخب وتعدد طرق إقناعه بطريقة جذابة ومستمرة ومتلاحقة، مما يؤدي إلى صياغة الرسالة الإعلامية عبر وسائل الاتصال الحديث بشكل جيد يستجيب معها متلقي تلك الرسالة ويتفاعل معها ويبدي رأيه في نوع من التغذية الاسترجاعية.

٦- الفضاء الالكتروني وتشجيع عملية التغير في النظم الاستبدادية

ولم تقتصر الاستفادة من الفضاء الالكتروني على الأفراد أو الأحزاب السياسية بل استفادت منها حركات المعارضة بشكلها الرسمي وغير الرسمي كأداة إعلامية جديدة لا تخضع للرقابة الحكومية، مع قدرتها على الانتشار والتأثير في الرأي العام وهذا ما يفسر درجة التأثير المرتفعة للانترنت في النظم المنغلقة عنها في النظم الديمقراطية، والتي كانت تتسم باحتكار الدولة لوسائل الإعلام التقليدية وتقليل هامش حرية التعبير داخل المجتمع وعدم فاعلية الأحزاب السياسية وغيرها من سمات النظم الدكتاتورية.

و أدت عملية التدفق الحر للمعلومات على إزالة الحواجز بين النظم السياسية وبعضها البعض بشكل أدى إلى تحول الإنترنت إلى سوق عالمي للأفكار الديمقراطية والترويج للأجندة الدولية لحقوق الإنسان وبما أدى إلى انفتاح المجتمعات المنغلقة على ثقافات أخرى ،ودرجة ما تتمتع به من الحرية والمستوى الاقتصادي والمعيشي بما فرض المزيد من الضغط على النظم السياسية القائمة لتلبية مطالب مواطنيها والذين أصبحوا يتطلعون نحو الأفضل ، وذلك مع تعدد ما أتاحه الإنترنت ادوات لحرية الحواروالتعبيرعن الرأي والمناقشات من خلال منتديات الإنترنت والمدونات وأنشطه المواقع والمجموعات البريدية واستطلاعات الرأي والتجمعات الافتراضية.[1]

وأصبح الموقف من حريات وسائل الاتصال والمعلومات والإنترنت تؤشر لدرجة انفتاح النظام السياسي نحو الديمقراطية، وعمل الإنترنت كمعارض سياسي من خلال جعل المعلومات أكثر انفتاحا على المجتمع، وتجاوز مساوئ المركزية، والمساعدة في انتشار فكرة وتجاوز الزمان والمكان وإتاحة الفرصة للتعبير والضغط على الحكومة، والقدرة على تغيير خطط تحقيقة بسرعة، والقدرة على امتصاص الضربات الأمنية والقمعية، واستفادت المعارضة السياسية الرسمية وغير الرسمية مما أتاحه الإنترنت من آليات للاحتجاج أوعبر حشد المواطنين للتفاعل مع قضية ما عبر المنتديات أو المجموعات البريدية أو غرف الدردشة أو التصويت الالكتروني على إحدى القضايا، أو رسائل المحمول، وأثرة على كفاءة التنظيم السياسي وسرعة الاستجابة للأحداث ومناهضة السياسة القمعية والحشد والتعبئة والتجنيد دون الحاجة بالضرورة لدعم خارجي .[2]

(1) عادل عبد الصادق:"الانترنت والاصلاح السياسي في مصر "، مرجع سابق ذكرة.
(2) مرجع سابق ذكرة .

٧- الفضاء الالكتروني و المساهمة في تفعيل دور المجتمع المدني

عملت تكنولوجيا الاتصال والمعلومات على المساهمة في تقوية مؤسسات المجتمع المدني سواء بقدرتها على التواصل مع مجتمعها سواء عبر مبادراتها أو مبادرة المواطنين الذين يصبح لديهم القدرة على الاتصال وبسهولة تكوين المنظمات الأهلية، وبشكل يزيد من القدرة على تحسين أداء المجتمع المدني والعمل على المحاسبية تجاه نفقاتها ومستوى تواصلها مع الجماهير، وتوافر لتلك المنظمات مواقع على الإنترنت يمكن من خلالها تفعيل الرقابة على سير العملية الانتخابية ومواقع منظمات المجتمع المدني التي تراقب سير العملية الانتخابية والأفراد الذين يستطيعون أن يبثوا ملاحظتهم عبر المدونات أو المواقع البريدية أو المنتديات أو الدردشة أو استطلاعات الرأي الالكترونية، وتلقي الشكاوى والمراسلات عبر البريد الالكتروني أو عبر الاتصال المباشر. و ساهم الفضاء الالكتروني في الكشف عن عددً من القضايا التي تتفاعل مع الشارع، وتعكس اهتمامات الحياة اليومية للفت الانتباه لدى تلك المنظمات الأهلية إلى قضايا معينة أو أماكن أصبحت بحاجة إلى مساعدة، بل وتطور هذا الدور لإنشاء منظمات مدنية للدفاع عن قضايا ما بناء على تأثير تكنولوجيا الاتصال والمعلومات، وأوجدت الحاجة لإيجاد كيان قانوني أو نقابي يدافع عن حرية الرأي والتعبير عبر الإنترنت كتلك التي تتعلق بالمدونات، ووفر الإنترنت أداه للتواصل والارتباط بين منظمات المجتمع المدني المحلي والعالمي.

٨- الفضاء الالكتروني وتعزيز المشاركة السياسية الرسمية وغير الرسمية:

تعرف المشاركة السياسية بأنها النشاط الذي يقوم به الأفراد بصفتهم الشخصية بهدف التأثير على القرارات الحكومية، أي أنه تعدى مجرد التصويت في الانتخابات أو العضوية في الأحزاب السياسية، ومن هنا تظهر قدرة المدونات في توسيع مفهوم المشاركة السياسية من خلال إعادة تعريف السياسي ليضم كافة التفاعلات اليومية المرتبطة بالتأثير على بنية القوة في المجتمع والتأثير على توزيعها، و كذلك في تكسير الحواجز بين العام والخاص، وبين النخبة والجماهير وبين الفرد والدولة.[1]

ويقوم المدونون بإنشاء قنوات خاصة خارج القنوات السياسية الرسمية العام، وبطريقتهم للتعبير عن آرائهم ومصالحهم، وما أتاحته من أدوات تعبير جديدة دور فاعل في المشاركة السياسية غير الرسمية وتمتعها بارتفاع سقف حرية التعبير بها، وكشفها لمشكلات بنيوية وتنظيمية وثقافية ودينية وقانونية داخل المجتمع وكونها أداة للتفاعل بين الفرد والمجتمع والدولة، وتأثيرها على طبيعة ونمط العلاقة بين مدخلات ومخرجات النظام السياسي وكذلك المساعدة في توسيع دور وعدد المشاركين في قضايا بناء الرأي العام، وتشكيل درجة الوعي السياسي المكون للفكر، وبما بجعل الأفراد لديهم المبادرة لتنمية معارفهم وأرائهم السياسية بنفسهم دون الركون بالضرورة إلى مؤسسات الدولة الرسمية والإعلام الحكومي. وبدأ الانتقال من حالة الرأي إلى إثارة الحوار والنقاش حول القضايا العامة في حوار يكون ذا طابع ندي، وهذا ما يصب في التأثير على الرأي العام و صانعي القرار وفي نفس الوقت يمثل ضغطا

(1) عادل عبد الصادق، " المدونات من الاحتجاج الشخصي إلى توجيه الرأى العام" مجلة تطبيقات مصرية، مركز الدراسات السياسية والاستراتيجية بالاهرام، العدد ٦٨، ٢٢ نوفمبر ٢٠٠٦ يمكن الاطلاع علية على الرابط التالي (http://acpss.ahram.org.eg/Ahram/2006/11/22/COMM0.HTM
(اخر زيارة ٢٠-١١-٢٠٠٨)

ورقابة على أداء الحكومة في آن واحد ، و تأسيساً على ذلك تتيح الإنترنت التواصل مع العالم بأكمله، وبالتالي ستتغير أيضاً بشكل حاسم عملية تشكيل الرأي العام. ومن الممكن أن يُحدث تطور كهذا نتيجتين مهمتين، وهما: الاشتراك العريض لقطاعات واسعة من المجتمع في بناء الرأي العام، وتبعاً لذلك مشاركة عامة أوسع في مراحل اتخاذ القرار.

وأدت الثورة التكنولوجية وما أتاحه الإنترنت من إمكانية مساهمة أي فرد في العملية السياسية إلى ظهور فاعلين جدد ولاعبين في الحياة السياسية ومن هؤلاء الأفراد الذين أصبحت لديهم القدرة على لعب دور الصحفي والإعلامي وكذلك المدونين والقراصنة الذي يقومون بدور في المجاهرة والاعتراض والمعارضة للنظام السياسي والتأثير على الأمن الالكتروني وبيئة تكنولوجيا الاتصال والمعلومات، وكذلك أتاحت مواقع التعارف الاجتماعية عبر الإنترنت لوجود تجمعات شبابية ليست فقط محلية بل أنها تعد دولية الطابع والتأثير حيث زيادة التعارف بين الشباب في العالم ومناقشة قضايا هامه وتنسيق المواقف حولها وجمع التبرعات كقضية الفقر ومكافحة الإيدز.

٩- ظهور أشكال جديدة للمعارضة السياسية وفاعلين جدد في العملية السياسية

ساعد الفضاء الالكتروني على المساهمة من قبل عدد كبير من المستخدمين للتعبير عن احتجاجهم ومشاركتهم وضغطهم على النظام السياسي الحاكم ، ويعد الاحتجاج شكلاً من أشكال الضغط غير العنيف على المؤسسات الحكومية أو الرسمية وذلك لتحقيق مطالب معينة ويأتي هذا الضغط في شكل إضراب عن العمل أو وقفات احتجاجية أو أي مظاهر احتجاج يتم الاتفاق عليها، وجاء التزاوج ما بين الاحتجاج كأداة للتعبير عن الرأي والإنترنت كوسيلة لدعم التنظيم والحشد والتعبئة والتجنيد والتنسيق والدعاية. ويأتي هذا في صورة تقديم المساعدة في الشكل التنظيمي والدعائي للاحتجاج التقليدي أو في وجود احتجاج يأخذ طابعا الكترونيا بحتا أو وجود احتجاج يجمع كلا النمطين، وهناك من يحتج على بعض المواد المنشورة عبر الإنترنت والمعادية وكذلك المطالبة بتغيير أوضاع أو سياسات أو احتجاج على اعتقالات أو إحداث بعينها ،وظهر ذلك في تناول بعض القضايا ذات البعد الدولي مثل القيام بحملات الكترونية لمقاطعه المنتجات الدنمركية أو الاحتجاج على ممارسات إسرائيل في الأرض المحتلة إلى الاهتمام بقضايا حياتية تعبر عن معاناة المواطن كارتفاع الأسعار وسياسات حكومية محددة. ويعمل الفضاء الإلكتروني كوسيط في إجراء الاتصالات بين مؤيدي الإضراب، وطرح إمكانية الاستفادة من خبرات شبابية على صلة بتكنولوجيا الاتصال والمعلومات، كما يتميز بدرجة عالية من المرونة والانفتاح على الأخر، في إطار من الرغبة في تحقيق المنفعة العامة، ويتيح الفرصة للتفاعل والاتصال المستمر بين منظمي الإضراب بما ينعكس على تطوير إستراتيجيتهم، وأيضا يتم توظيف الإنترنت في نشر المعرفة والوعي بالقضية محل الاحتجاج، وتوفير وسيط إعلامي سريع الانتشار ورخيص التكلفة وفي متناول فئة عريضة من الشباب عير تشكيل مجموعات على موقع الفيس بوك أو المواقع الاجتماعية والمدونات ورسائل المحمول المجانية.[1] ومن أهم صور الاحتجاج جمع

[1] Robert Klepper, "The World Wide Web as Mass Medium," Information Strategy 14 (Fall1997): 1 [database on-line]; available from Wilson Web; accessed 18 January 2007.

التوقيعات الالكترونية للمطالبة بتغيير سياسات أو قرار أو إزالة صور تعد مسيئة أخلاقيا أو دينيا، والدخول إلى غرف الدردشة والمنتديات في الإنترنت للقيام بحوارات وتكوين رأي مناصر أو مناهض لقضية من القضايا؛ وتكوين التحالفات السياسية في الإنترنت، ورسالتهم بنشر أفكار الإضرابات أو الاعتصام بين أكبر عدد من مستخدمي الإنترنت عن طريق المجموعات البريدية ورسائل المحمول، و مهاجمة المواقع الحكومية الالكترونية أو مواقع الخصوم والقرصنة وسرقة المعلومات ونشر الفيروسات وغيرها. وإرسال كم كبير من الرسائل الاحتجاجية لكافه الأطراف المعنية بصورة ضاغطة ومزعجة عن طريق البريد الإلكتروني، وإنشاء مواقع انترنت لنشر الأفكار والرؤى الخاصة بالموقف الاحتجاجي للحصول على تأييد الرأي العام وتجنيد الموالين والداعمين لفكرة الاحتجاج من جماعات المصالح المختلفة. وتعكس أدوات الرأي والتعبير عبر الإنترنت كالمدونات والصحافة الالكترونية نوعاً من التغذية الاسترجاعية تجاه القرارات الحكومية، ومن ثم فان كفاءة النظام السياسي تتوقف على قدرته لتلبية هذه المطالب.

١٠- دور الفضاء الالكتروني في جودة الأداء الحكومي والحكم الصالح والنمو الاقتصادي.

كان من استخدام تكنولوجيا الاتصال والمعلومات ومن ضمنها الإنترنت في الإدارة الحكومية دور في ظهور مفهوم الحكومة الالكترونية الذي أصبح يؤثر على عمل ووجود الحكومة الكلاسيكية مع قدرتها على الاندماج الهائل في محيطها الاقتصادي والاجتماعي في ظل الدخول في مجتمع المعلومات بالترافق مع تغييرات مؤسساتية واستقدام لخبرات ومهارات إضافية بما يؤدي لتحسين الخدمات العامة وتعزيز الإجراءات الديمقراطية، ويقدم الدعم اللازم للسياسات الحكومية، وكان من الحكومة الإلكترونية كوسيلة لتمكين الحكومة من تأثير إيجابي في تأمين إدارة أكثر كفاءة لمواردها. وبالتالي تمكينها من تنفيذ سياساتها وخططها بكفاءة مرتفعة. والمساهمة في رفع جودة المعلومات وتبسيط طرق الوصول إلى المعلومات، وتخفيض كبير في زمن إنجاز المعاملات، و في أعباء الحصول على الخدمات الحكومية، و تخفيض كلفة تقديم الخدمة العامة، ورفع مستوى تقديمها و رفع الكفاءة و تحقيق رضاء المواطن، وانعكاس ذلك على عملية التنمية وقدرة المواطنين على الوصول إلى المعلومات بشكل أسهل. وهذا يؤدي لنشوء علاقة ثقة بين المواطن والحكومة، و تحفيز التحول الالكتروني للمجتمع وإيجاد حالة من الحوار بين الجهاز الحكومي وأفراد المجتمع بما يؤدي إلى رفع كفاءة السياسات الحكومية و تحسين القدرة التنافسية للاقتصاد واستقطاب رؤوس الأموال والاستثمارات. وساعد الإنترنت في التوجه نحو الحكم الجيد والرشيد عبر برامج الحكومة الالكترونية والتي تعمل على الحد من الفساد الإداري والبيروقراطية وترشيد النفقات الحكومية، والقدرة على استيعاب مطالب المواطنين من خلال توفير تلك النفقات في تحسين نوعية الخدمة وسرعتها، وبما يعمل على تشجيع الاستثمار الأجنبي والمحلي بشكل يظهر في النمو الاقتصادي.[1]

(1) عادل عبد الصادق، الانترنت والاصلاح السياسي في مصر " مرجع سابق ذكره .

# الفصل الثاني :

## إشكاليات مفهوم الإرهاب الالكتروني والمفاهيم ذات الصلة

## الفصل الثاني:
## إشكاليات مفهوم الإرهاب الالكتروني والمفاهيم ذات الصلة

على الرغم من تميز الإرهاب الالكتروني في مفهومة وخصائصه والياته إلا انه يثير مجموعة أخرى من المفاهيم والتي ان اختلفت عن الارهاب الالكتروني فانها -في الوقت ذاته - ترتبط بدرجة او باخرى كما هو الشأن بالنسبة الى الجريمة الالكترونية وحرب المعلومات والمقاومة الالكترونية والاحتجاج الالكتروني وهو ما نعرض له في ثلاثه مباحث تتناول اولها تأصيل ماهية مفهوم الإرهاب الالكتروني و بيان سماته وخصائصه ، بينما يتناول المبحث الثاني هجمات الفضاء الألكتروني ما بين توصيف الإرهاب ومدلول الحرب ، ويتناول المبحث الثالث المفاهيم المرتبطة والمتداخلة مع الإرهاب الالكتروني

# المبحث الاول:
# هجمات الفضاء الالكتروني
# ما بين توصيف الارهاب ومدلول الحرب

**ثار الجدل واحتدم الخلاف حول طبيعه هجمات الفضاء الالكتروني وما اذا كانت تشكل ارهابا ام حرباً من حيث طريقة الفعل والتنفيذ ويعالج ذلك الباحث من خلال ثلاثة مطالب يتناول المطلب الاول مفهوم الحرب ومجالها وادواتها بينما يركز المطلب الثاني على تناول مفهوم الحرب غير المتماثلة، وأما الثالث فيتناول هجمات الفضاء الالكتروني ومفهوم الارهاب، وذلك على النحو التالي :**

## المطلب الاول:
## ظهور الإرهاب الجديد: التزاوج ما بين التكنولوجيا والإرهاب

برزت ظاهرة جديدة تمثلت في قيام العولمة المتزامنة مع الجريمة والإرهاب و توجّه الإرهابيون نحو الجريمة لدعم نشاطاتهم، وتوثقت العلاقة بين الجريمة والإرهاب بشكل يتعدى الفهم التقليدي القاضي بان المجرمين يمارسون الجريمة لمجرد الربح المادي، وأصبح الإرهابيون يعملون بصورة حصرية لتحقيق أهداف سياسية ولقد أدت التطورات التكنولوجية وما أضافته من تعقيد على طبيعة الفعل إلى حدوث التداخل ما بين الإرهاب والجريمة، وكان لشبكات تكنولوجيا الاتصال والمعلومات دورها في عملية تحول الإرهاب إلى تهديد عالمي الطابع وأصبح جريمة عابرة للحدود القومية من حيث النشاط والخطط والتمويل، وأدى ذلك إلى إرباك الأنظمة القانونية للدول التي تُستخدم كأداة لمكافحة أنماط تلك الجرائم في كافة اشكالها، وينقل الإرهابيون والمجرمون الناس، والأموال، والسلع بما يوفر غطاء مميزا لنشاطهم، وجاء ذلك بعد تطور طبيعة التهديدات للأمن الدولي.

وفي فترة ما بعد الحرب الباردة كانت النزاعات بين الدول القومية بمثابة التهديد الرئيسي للأمن الدولي، وبناءً على ذلك، كانت الدول قادرة على التحكّم بالأمن الدولي ولكن تغيرت الطبيعة الأمنية وظهرت تهديدات جديدة غير تقليدية كان منها عمليات الشبكات الإجرامية والإرهابية التي مثلت تهديدا للأمن الدولي بفعل الثورة المعلوماتية والتكنولوجية، ويمثل الإرهاب الجديد الجيل الثالث في تطور الظاهرة الإرهابية في العصر الحديث فالجيل الأول كان عبارة عن موجات إرهاب ذات طابع قومي متطرف التي اجتاحت أوروبا في أواخر القرن ١٩ وحتى عقد الثلاثينيات، أما الجيل الثاني فكان إرهابا ذا طابع ايدولوجيا أثناء الحرب الباردة وكان أداة من أدوات الصراع بين الشرق والغرب.

ونشأت العديد من الحركات الإرهابية في أوربا الغربية، أما الجيل الثالث فيتسم بخصائص مميزه ومختلفة عن الأجيال السابقة من حيث التنظيم والتسليح والأهداف، ويتسم جماعات الإرهاب الجديد بغلبة النمط العابر للجنسيات حيث يضم أفراد من جنسيات مختلفة ولا تجمعها سوى قضية قومية أو دينية وأيدلوجية وبنية دوافع وأسباب محددة، ولديها القدرة على الانتقال من مكان إلى أخر ويصعب متابعتها، ويكون هدف هذه الجماعات هو إيقاع أكبر اثر ممكن على الأعداء وليس مجرد مدى

تحقيق المطالب السياسية، وأصبح الإرهاب الجديد يضم أفراداً على درجة عالية من الكفاءة التكنولوجية تمكنهم من استخدام منظومات تسليحية أكثر تعقيداً. (1)

ففي مارس ١٩٩٥ وقبل خمس سنوات من الأحداث الإرهابية في الحادي عشر من سبتمبر ٢٠٠١ حدث هجوم في مترو الأنفاق في طوكيو باستخدام غاز السارين قامت به جماعه الحقيقة المطلقة المتطرفة حيث أدى إلى قتل ١٢ شخصا وجرح ٥ آلاف، ومثل ذلك نقلة نوعية في تطور العمل الإرهابي وأصبحت الجماعات الإرهابية خارج سيطرة الدولة ،وتم استخدام المنجزات التكنولوجية في الإرهاب، والتي من خلالها يستطيع الإرهابيون تحقيق إنجازات والحاق أضرار غير متوقعه ومن ثم أصبحت الجماعات الإرهابية تمثل تهديداً للدول بدرجة تفوق تهديد الدول لبعضها البعض. (2)

وأصبحت التكنولوجيا من الوسائل الداعمة للعمل الإرهابي، والمساهمة في زيادة ديناميكيته وسهولة انتشاره وتعاظم أثره وذلك على اعتبار أن التكنولوجيا هي "مجموعة المعارف والأساليب المتاحة واللازمة للإنتاج والتنمية في كل عصر من العصور " أما تكنولوجيا الإرهاب فتشتمل على جانب (مادي) يتمثل بالمواد والأدوات والتجهيزات والوسائل التي يستخدمها الإرهابي أو يصنعها؛ وجانب آخر (عقلي) يتمثل بالمعارف والخبرات والأساليب اللازمة لتعامل الإرهابي مع بيئته المحيطة، ولاستخدامه أو تصنيعه للجانب المادي من التكنولوجيا. (3)

وقد شهد القرن العشرون العديد من التطورات التكنولوجية والتي شملت المجالات السلمية وغير السلمية حيث شمل الجانب السلمي في التطور في الاتصالات والموصلات، والراديو والتلفزيون، والرسائل المكتوبة، والاتصال عبر الأقمار الاصطناعية، والكمبيوتر بأجياله المتعددة، وشبكة الاتصالات العالمية (الإنترنت)، وكذلك المواصلات البرية والبحرية والجوية، وصولا إلى استخدام تلك التكنولوجيا في الأغراض العسكرية في شكل ثورة في الشئون العسكرية والتطور في الأسلحة الخفيفة، والمتفجرات، وأسلحة الدمار الشامل بأنواعها: الكيميائية والبيولوجية والنووية؛ وإن كانت أغلب الانجازات الحضارية التكنولوجية قد بدأت كاستخدام عسكري كالأثر الذي أحدثه اكتشاف الصواريخ والإنترنت وغيرها، ،وأصبح هناك مراحل وعمليات تقوم بها المجموعة الإرهابية باعتبارها أبرز الملامح النظرية لتكنولوجيا الإرهاب. (4)

وحدت تكنولوجيا الاتصالات الحديثة من تأثير المسافة والزمن وسهلت من انتقال المعلومات والأفكار والاتجاهات في زمن قياسي إلى أبعد مكان، وهي مميزات استغلها الإرهابيون في تحسين الاتصال بين بعضهم البعض بهدف تدفق الدعم، والتنسيق مع الأتباع، والوصول إلى جمهور ضخم من

---

(1) Dan Verton,. **Black Ice: The Invisible Threat of Cyber-Terrorism.** New York, McGraw-Hill/Osborne, 2003. p. 273 .

(2) Thomas Mockaitis," The "New" Terrorism: Myths and Reality", Middle East Quarterly VOL,XIV,No, 4, Fall 2007.

(3) زكريا حسن أبو دامس،" اثر التطور التكنولوجي على الإرهاب"، رسالة ماجستير(منشورة ) ، قسم العلوم السياسية في الجامعة الأردنية، ٢٠٠٥م ،والتي صدرت ككتاب بعنوان " اثر التطور التكنولوجي على الإرهاب " ، الطبعة الأولى ، ٢٠٠٥ عن دار (عالم الكتب الحديث) ودار (جدار للكتاب العالمي) للنشر والتوزيع بالأردن،

(4) زكريا حسن أبو دامس، مرجع سابق ذكره.

المتعاطفين المحتملين، وتجنيد أعضاء جدد فوق رقعة جغرافية ضخمة، ويمكن ملاحظة أن الجماعات الإرهابية القديمة تحددت بعامل المكان في دولة معينة، وكانت الادوات تتمثل في التفجيرات أو الغازات السامة أو الاختطاف ، وكانت دوافعها ذات عنصر محلي إلى حد كبير كالسعي للانفصال أو المطالبة ببعض الحقوق أو من خلال العمل كجناح عسكري سري ضمن حركه سياسية، أو حركه مقاومه محلية، وتميزت تلك الجماعات بان طريقتها في العمل كانت أكثر أحاديه تجاه استخدام العنف والقتل.

وتميزت الجماعات الإرهابية بان قدرتها على التجنيد والتمويل محدودة وكانت أعمال تلك الجماعات موجهة في أغلبها ضد الحكومات فقط وكانت قدرتها على التواصل مع العالم الخارجي محدودة وكذلك مخاطبة الرأي العام، ومع دخول عنصر الكمبيوتر في عمل تلك الجماعات الإرهابية التقليدية نجد آثارا مهمة ومشكلات جديدة وبدا نطاق الإرهاب يتغير بإضافة الكمبيوتر فلم يصبح المنفذ للعمل الإرهابي الجماعة فقط، ولكنها استطاعت أن تكسب أشخاصاً جدداً، كجماعه التاميل أصبحت لا تعمل فقط في سريلانكا بل في أمريكا واستراليا ولندن وغيرها وكذلك جماعه الحقيقة في اليابان، أما بالنسبة لطريقه الفعل فقد أصبحوا يستخدمون العنف والتهديدات والتجنيد واتسع مجال التدريب ووضع الاستراتيجيات، أما بالنسبة لأدوات التنفيذ فلم تعد قاصرة على عمليات قتل أو اختطاف بل تعدت ذلك إلى مرحلة التجنيد والدعاية المضادة.[1]

وبهذا مثل دخول الإنترنت والكمبيوتر في مجال الإرهاب التقليدي تغيرا حقيقيا في عناصر ومشكلات الظاهرة ولم يعد ينطبق عليها التعريفات القديمة للإرهاب وينبع من هذا صعوبة مواجهتها بالطرق التقليدية، خاصة مع النمو المتسارع في النمو التكنولوجي بشكل لا يتواكب معه طرق المواجهة التي غالبا ما تكون عاجزة والتي تبقى محصورة في الغالب في حالة رد الفعل فقط،ويسعى الإرهاب الجديد الى خدمة البعد الإعلامي والعسكري لأهدافه حيث يتم الأول عبر استغلال كافة الجماعات' المتطرفة' الأصولية علي اختلاف أشكالها مزايا الإنترنت كعنصر حيوي لدعم وتحقيق أهدافها ومنفذ لوجستي داعم وحاضن لنشاطها الإعلامي في مناطق مختلفة من العالم حيث أصبحت تلك الجماعات لا يهمها كم من الناس قتلوا بقدر ما يهمها بكم من الناس شاهدوا وتفاعلوا مع الحادثة الإرهابية، وتحول أفراد الإرهاب من مجموعة قليلة من الناس موزعة جغرافيا لتشكل مجتمعا خاصا بها يساعدها علي الالتحام والتواصل الدائم، الأمر الذي يوهم البعض بأن هذا المجتمع غيرمحدد كميا[2]

وظهرت العلاقة بين تطور الوسائل التكنولوجية وتطور العمل الإرهابي وانعكس ذلك في درجات الخطر الذي يمثله وتحديات المواجهة، وقد تمكنت الجماعات الإرهابية والأخرى ذات الدوافع الدينية من التهديد باستخدام أسلحة الدمار الشامل خاصة مع انهياربعض النظم والدول الفاشلة والتي أفرزت ما يطلق علية السوق السوداء للمكونات النووية والبيولوجية بعيداً عن سيطرة الدول، وأصبح العالم أمام ما يمكن أن يطلق علية "العصر الجديد للإرهاب " وذلك بالمقارنة بتغير ملامح وخصائص وتداعيات الإرهاب القديم التقليدي في مواجهه ظهور ملامح "الإرهاب الجديد " Super Terrorism " ذلك الارهاب

---

(1) Adam Roberts," **The Changing Faces of Terrorism"**, BBC History: 2002-08-27.

(2) عادل عبد الصادق ،" **مكافحة الإرهاب عبر الإنترنت .. التحديات والفرص** "، دراسات سياسية، جريدة الأهرام، ١٦-٦- ٢٠٠٧ .

المفرط في تقدمه، وجاء دور الفضاء الالكتروني في تحول الجماعات الإرهابية من الطابع القومي إلى طابع عابر للقوميات حيث أصبحت لا تتقيد بحدود الدولة بل أنها تعمل على نطاق عالمي وتسعى إلى التأثير الكوني لأعمالها ومخاطبة الرأي العام كما وفر التقدم التكنولوجي من وجود آفاقاً جديدة للعمليات السرية، و تميزت بتعدد الجنسيات المنضوية تحت عمل تلك المنظمات، كما أن تلك المنظمات تعمل من خلال بنيان شبكي لا مركزي، كما أن هناك إمكانية للتنسيق والتجنيد والتعبئة والتمويل عبر شبكات تكنولوجيا الاتصال والمعلومات والهاتف المحمول وأجهزة الكمبيوتر المحمولة والبريد الالكتروني ومواقع الإنترنت [1].

وادى ذلك للكشف عن الأهداف المعرضة للخطر أكثر من الكشف عن الإرهابيين أنفسهم، وفرض ذلك التحول في شكل الإرهاب اختلافا في درجات المواجهة والمكافحة ومحاولات فهم طرق وأساليب الإرهاب الجديد ودوافعه وأهدافه في التحكم في التكنولوجيا، وبشكل جعل العالم أمام ثورة في الإرهاب بالتركيز على التكنولوجيا وأسلحة الدمار الشامل، ففي العقد الأخير شهد الإرهاب الجديد تغيرا في طبيعته وخصائصه، وارتبطت فكرة الإرهاب بالحرب غير المتماثلة.

ويعرف الإرهاب من قبل كل دول العالم على انه جريمة لكي يتم التعامل معه جنائيا ويكون لتحقيق اهداف سياسية، وهناك من الدول من تمارس الإرهاب على شعوبها، وكان للفاعلين الجدد باستخدام التكنولوجيات الجديدة والتكتيكات دور في التأثير دون شك في تغير طبيعة الإرهاب، وقد يدفع غموض دور الفاعلين في الإرهاب وممارسته إلى خوف الدول من إن تستخدم دول أخرى الإرهاب ضدها وبشكل يكون أكثر فاعلية من ممارسة الأفراد والجماعات له، تحول الإرهاب من كونه تكتيكاً إلى إستراتيجية فرض تحديات لمواجهه ذلك الإرهاب.[2]

وشكلت التكنولوجيا قاطرة التغيير في الشكل العملي للإرهاب ليعكس تغييرات في التنظيم والمبادئ والتقنية المستخدمة والاستراتيجية وفي الفاعلين وهناك مؤشرات على ذلك منها زيادة عدد الجماعات الارهابيه التي تطبق الأشكال التنظيمية التي تعتمد على تكنولوجيا المعلومات لدعم هياكلها، وكانت الجماعات الجديدة التي تأسست في الثمانينات والتسعينات أكثر استخداما للتكنولوجيا من الجماعات التقليدية، ووجود علاقة ايجابية ارتباطيه بين درجة نشاط أي جماعه ودرجه اعتمادها على تكنولوجيا المعلومات للدعم التنظيمي ولأغراض الهجوم، ويتوقع أن تعتمد الأجيال الجديدة من هذه المنظمات عليها بصورة اكبر في المستقبل.

وظهر نوع جديد من حروب العصابات تمزج فيه الجماعة الإرهابية بين حربها المادية على الأرض مع حربها الإلكترونية عبر الفضاء الالكتروني، إضافة إلى استخدامه كأداة ووسيلة اعلامية مثلى لبث دعواهم إلى جمهور أوسع بحرية تامة بعيد نسبياً عن سيطرة الحكومات والرقابة الإعلامية ومن دون الكشف عن هوياتهم، مع تحسين عملية الاتصال بين المنظمات الإرهابية بعضها البعض مما يخلق جبهة

---

(1) Jeremy Pressman,"Rethinking Transnational Counterterrorism ", The Washington Quartery, Vol.,30,No.4,Autumn 2007 .
(2) Matthew J. Morgan," The Origins of the New Terrorism", Parameters, Vol. 34, Spring 2004,pp 29-43

إرهابية شبه موحدة ويقوي الشعور بالتضامن في وجه "العدو المشترك". وكان الإرهاب تاريخيا يعتبر ظاهرة تكتيكية والتي تتعامل مع الجغرافيا والثقافة والتي كان لا يمكن تحديدها بدقة حيث كان الإرهاب أداة للثوريين والقوميين و كان من الممكن إن يستخدم من قبل الدولة كوسيلة للإبقاء على سلطتها ومن ثم كان نعت الشخص أو المجموعة بأنها إرهابية فيه شيء من الحكم الأخلاقي وهي ما يقودنا إلى مشكلة اكبر في التعريف، فحتى دعاة الحرية قد يستخدمون الإرهاب كتكتيك مع ان ذلك قد لا يساعد على شرعيتهم [1]

وفي الماضي كانت الحروب في صورتها العامة عبارة عن مجموعه من الأعمال الإرهابية المنظمة كما في حالة الحرب الأهلية والحروب الثورية وحروب التحرير الوطني، ويرى الإرهابيون أنفسهم وأعمالهم كرد فعل للهدف والسبب الذي يقودهم ويدفعهم لاستخدام القوه لتحقيق أهدافهم في مواجهه القوة الشاملة للدولة ، وظهرت ملامح ارهاب جديد يستخدم التكنولوجيا ويتمتع بقوة كبيرة في التنفيذ والتخطيط ، ففي تفجيرات مدينة ممباي العاصمة الاقتصادية للهند في ٢٦ نوفمبر ٢٠٠٨ ، والتي أدت إلى مصرع ١٩٥ وجرح ٣٠٠ شخص تم التخطيط للعملية عبر أدوات تكنولوجيا الاتصال والمعلومات والاستعانة ببرنامج "جوجل ايرث" لتحديد الشوارع والتدريب وإجراء الاتصالات عبر الأقمار الصناعية والاستعانة بالانترنت في معرفة كيفية صنع المتفجرات، وليعبر ذلك عن نموذج للإرهاب الجديد، حيث تمكن زهاء ١٠ أفراد من السيطرة على المدينة في دقائق معدودة وضرب فندق تاج محل واوبروي وناريمان هاوس وهي العملية التي تبنتها منظمة عسكر طيبة المعادية للهند. [2]

وقد أوجد الفضاء الإلكتروني بيئة دولية جديدة تمثلت في:

١ـ اعطت البيئة الإلكترونية الجديدة وتكنولوجيا المعلومات دفعة لزيادة المعرفة في عمليات الإنتاج والابتكار، وأصبحت المنافسة الاقتصادية جزءا من المنافسة الأمنية، وأصبح الدخول في عصر الفضاء أحد أوجه هذه المنافسة.

٢ـ الاهمية المتزايدة للاتصالات وهي أحد أوجه الأمن مما جعل هذه البيئة الإلكترونية حقيقة غير مسبوقة، وقد فتح هذا المتغير الطريق أمام ظهور فاعلين جدد مثل القنوات الفضائية التي تعتمد على الناحية الفنية وتجنب الإعلانات التقليدية من أجل جذب جمهور واسع وتحول إلى مصدر حقيقي للمعلومات وصانعي القرار مما يعكس الدور المتزايد للمجتمع المدني العالمي وتراجع الدولة كفاعل رئيسي في العلاقات الدولية، ويختلف دور هذه المنظمات من دولة إلى أخرى كما أن تأثيرها يرتبط ببيئتها السياسية والاقتصادية والاجتماعية وقد تمتعت هذه المنظمات بتأييد الحكومة لأنشطتها. ٣ـ عدم كفاية الاعتماد على القوة العسكرية، فالأمن لا يأتي من خلال السلاح، فالاقتصاد والاتصالات أديا إلى ظهور تعريف جديد للأمن؛ وظهور أوجه غير عسكرية له، وأصبحت حقيقة التهميش المتزايد من الاقتصاد العالمي ظاهرة تعاني منها دول العالم مع الآثار الاقتصادية السلبية للعولمة.

---

(1) Alexander Spencer, Questioning the Concept of 'New Terrorism', Peace Conflict & Development, Issue 8, January 2006.

(2) جريدة الشرق الاوسط، ٣ ديسمبر ٢٠٠٨ .

## المطلب الثاني :
## هجمات الفضاء الالكتروني ومفهوم الارهاب

أولا :الجدل العالمي حول تعريف الإرهاب

يعتبر"تعريف الإرهاب" واحدا من الإشكاليات الأساسية التي تسيطر على النقاش العام حول تلك الظاهرة على المستوى الدولي ، والتي يعتقد على نطاق واسع أنه يعرقل " التوافق الدولي" المطلوب لعقد مؤتمر عالمي حوله، كما يؤدى إلى إرباك التعاون الدولي في مكافحته، إضافة إلى ما يثيره من خلافات واسعة بين الدول العربية والقوى الكبرى حول قضايا جوهرية تتعلق بما يعتبرارهابا ومالا يعتبركذلك .

هناك فرق بين الإرهاب كظاهرة إجرامية والإرهاب كظاهرة قانونية، وتستمد الظاهرة الإجرامية طبيعتها من تأثيرها في المجتمع وتعالج بوسائل مختلفة منها الوسائل الأمنية والاجتماعية والقانونية، وترتبط بالبواعث أو الأسباب التي تؤدي إلى الإرهاب كما ترتبط بتأثيرها في الاستقرار والأمن الداخلي والأمن والسلم الدوليين فضلا عن مساسها بقيم الديموقراطية وحقوق الإنسان، وتتحدد الظاهرة القانونية في ضوء ما يراه القانون الدولي لضبط أحكام الظاهرة الإجرامية لكي تقع تحت طائلة وفقا للضوابط التي يحددها ولا تتطابق بين عناصر الظاهرة الإجرامية والظاهرة القانونية، فالأولى تحكم من خلال نظرة جانب من المجتمع أو نظرة سياسية معينة، وتقع جريمة الإرهاب في نطاق القانون الجنائي الوطني والدولي معا ولو كان ذلك تحت وصف قانوني مختلف. [1]

ويتكون تعريف الإرهاب من مكونين أحدهما مادي يتمثل في إلحاق الأذى بالحق في الحياة والحق في سلامة الجسم أو الملكية الخاصة وحقوق ومصالح أخرى عامة تختلف من تعريف لأخر، وأما الركن الثاني للإرهاب فهو معنوي وهو أن يتوافر مصدر خاص يتراوح ما بين إحداث الرعب لدى الناس أو حمل دولة أو منظمة دولية على القيام بعمل أو الامتناع عن القيام بأمر ما، وتتمثل الأفكار السائدة بشأن " التعريف" في نقطتين :

الأولى، أنه لا يوجد تعريف متفق عليه بين دول العالم لما هو مقصود بالإرهاب، وأن الأمم المتحدة لم تتمكن لفترة طويلة من التوصل إلى توافق نهائي بهذا الشأن، وتم تجنب التطرق إلى ذلك في السنوات الأخيرة، والثانية، أن هناك اختلافا جوهريا بين ما يعتبر إرهابا وما يعتبر مقاومة مشروعة في حالات الاحتلال، كما أن هناك ما يمكن اعتباره إرهاب دولة يرتبط بممارسات غير تقليدية عنيفة لبعض الدول.[2] لكن ثمة اتجاهاً مهاماً يوجد توافق نسبى بشأنه يستند على إمكانية وضع معايير معينة أو " روابط" يمكن من خلالها تحديد المقصود بالعمل الإرهابي، كأساس للتعريف، وهي:الفعل المتبع، بمعنى استخدام العنف أو التهديد به سواء كان داخليا أو دوليا. و الرغبة في تحقيق أهداف سياسية ( إلقاء الرعب أو هدف ما) وفقا لنية مرتكب العنف. بالإضافة إلى وجود قصد خاص أو باعث لارتكاب العمل الإرهابي وجاء هذا الإرهاب ليتزاوج مع التكنولوجيا في شكل الإرهاب الجديد.

---

(1) د. احمد فتحي سرور ،" المواجهه القانونية للارهاب "، مركز الاهرام للترجمة والنشر ، الطبعه الاولي ، القاهرة ، ٢٠٠٨ ،ص ص ١٣-١٢٣ .

(2)د. احمد فتحي سرور ،" المواجهه القانونية للارهاب "، مرجع سابق ذكرة ،ص ص ٣٤-٥٦.

وقد مثلت ١١ سبتمبر ٢٠٠١ نقلة نوعية في تطور الإرهاب الجديد وأصبحت نقطة تحول في النظام الدولي وشكلا من أشكال الصراع المسلح على الساحة الدولية لدرجة أصبح يمثل بديلا للحروب التقليدية[1] وفي التقرير الصادر عن وزارة الخارجية الأمريكية في أكتوبر سنة ٢٠٠١ أن الإرهاب يعني: "العنف المتعمد ذا الدوافع السياسية، والذي يرتكب ضد غير المقاتلين وعادة بغية التأثير في الجمهور، حيث إن غير المقاتلين هم المدنيون، إلى جانب العسكريين غير المسلحين، أو الذين هم في غير مهماتهم وقت تعرضهم للحادثة الإرهابية أو في الأوقات التي لا توجد فيها حالة حرب أو عداء..."، وتعرف وكالة التحقيقات العدلية الأمريكية (FBI) للإرهاب بأنه: استعمال - أو التهديد باستعمال - غير مشروع للعنف ضد أشخاص أو ممتلكات لتخويف أو إجبار حكومة أو المدنيين كلهم أو بعضهم لتحقيق أهداف سياسية أو اجتماعية.

وفي قاموس أكسفورد نجد كلمة إرهاب (Terrorism) تعني سياسة، أو أسلوبًا يعد لإرهاب وإفزاع المناوئين أو المعارضين لحكومة ما. فالإرهابي(Terrorist) هو الشخص الذين يحاول أن يدعم آراءه بالإكراه أو التهديد أو الترويع. أما الإرهاب وفق الأمم المتحدة فيعني: "أعمال العنف الخطيرة التي تصدر من فرد أو جماعة بقصد تهديد الأشخاص أو التسبب في إصابتهم أو موتهم، وسواء كان يعمل بمفرده أو بالاشتراك مع أفراد آخرين ويوجه ضد الأشخاص أو المنظمات أو المواقع السكنية أو الحكومية أو الدبلوماسية أو وسائل النقل والمواصلات وضد أفراد الجمهور العام دون تمييز أو الممتلكات أو تدمير وسائل النقل والمواصلات بهدف إفساد علاقات الود والصداقة بين الدول أو بين مواطني الدول المختلفة أو ابتزاز أو تنازلات معينة من الدول في أي صورة كانت. لذلك فإن التآمر على ارتكاب أو محاولة ارتكاب أو الاشتراك في الارتكاب أو التحريض على ارتكاب الجرائم يشكل جريمة من جرائم الإرهاب الدولي".

وباستعراض هذا التعريف الأمريكي وغيره من التعريفات في الدراسات الغربية يتبين أن القاسم المشترك فيها هو استخدام العنف والقوة والغدر، ويتفق الجميع أن الإرهاب هو الاستعمال المطلق للعنف والقوة تجاه المدنيين أو الأهداف المدنية، أو العسكريين، أو الأهداف العسكرية في غير حال الحرب المعلنة بين طرفين بهدف بث الرعب بدون إنذار سابق. وإن إحدى المشكلات الرئيسية في هذا التعريف الكلاسيكي للإرهاب هي أنه تعريف منحاز أساسا إلى الدولة ضد الجماعات التي لا دولة لها. ويعكس هذا التحيز حقيقة أن الدول كان ينظر إليها عبر التاريخ باعتبارها تملك حقوق سيادة كاملة لكي تفعل ما تريد ضمن حدودها وداخل أراضيها دون اعتبارها مخالفة للقانون الدولي. لكن هذا التمييز ظل يزداد ضعفا على مدى العقود القليلة الماضية[2].

ويتطلب الإرهاب المحلي توافر عده خصائص و اختلافات أهمها يتعلق بأن ينتمي المشاركون في العمل الإرهابي وضحاياهم إلى جنسية نفس الدولة التي وقع فيها العمل الإرهابي، وان تنحصر نتائج

---

(1) احمد إبراهيم محمود " الإرهاب الجديد :الشكل الرئيس للصراع المسلح في الساحة الدولية " ، مجلة السياسة الدولية ، العدد ١٤٧ يناير ٢٠٠٢ ، ص ص ٤٤-٥٣.

(2) جراهام فولر، " نحو تعريف موحد للإرهاب"، الجزيرة نت ،٣-١٠-٢٠٠٤.

العمل الإرهابي في داخل حدود الدولة نفسها، وأن يتم الإعداد والتخطيط للعمل الإرهابي في نطاق السيادة القانونية والإقليمية للدولة، وألا يكون هناك أي دعم مادي أو معنوي لذلك النشاط من الخارج، ويخضع هذا النوع من الإرهاب المحلي للاختصاص والقانون المحلي الداخلي دون تدخل قانوني خارجي.

ويتعلق الإرهاب الدولي بتوافر اختلاف جنسيات المشاركين في العمل الإرهابي، وتباين جنسيات الضحايا، وميدان حدوث العمل الإرهابي يخضع لسيادة دولة ليست الدولة التي ينتمي إليها مرتكبو العمل الإرهابي، ووقوع العمل الإرهابي ضد وسائل نقل دوليه، وتجاوز الأثر المترتب على العمل الإرهابي نطاق الدولة الواحدة، وتباين المكان والتخطيط للعمل الإرهابي عن مكان التنفيذ، ووقوع العمل الإرهابي بتحريض من دولة ثالثة.[1]

وقد ذهبت لجنة الخبراء المنبثقة عن الاتحاد الدولي لتوحيد القانون الجنائي الى إن الإرهاب يكون دوليا في حالة إثارة الاضطرابات في العلاقات الدولية، وتوجه الجريمة ضد دولة غير الدولة التي فيها اعتداء الجريمة، وان يكون الفاعلون لاجئين من الخارج، وان يتم التجهيز للجريمة من دولة أخرى خلاف الدولة التي جرى بها العمل الإرهابي، ولا يخضع هذا النوع إلى الاختصاص الداخلي للدولة، وهناك أنماط للإرهاب وفقا لطبيعة النشاط كالإرهاب الثوري والإرهاب الانتحاري والفكري والنفسي والتي أخذت في التطور في ظل بيئة دولية جديدة تميزت بتحولات في النظام الدولي والثورة في الشئون العسكرية والعولمة الاتصالية وما فرضته من تحديات وطبيعة العلاقة بين النظم الحاكمة وجماعات المعارضة والهيمنة الأمريكية، وكان هناك علاقة واضحة بين العولمة والإرهاب حيث استفاد الإرهاب بما أتاحته العولمة من حرية التنقل والعمل والتكنولوجيا.

<u>ثانيا تنازع التكييف القانوني للإرهاب واقع الامر ان التكييف القانوني للارهاب تتنازعه ثلاثة وجهات نظر يكون للارهاب وصفا معين لدى كل منها على النحو التالي</u>

١- : <u>الإرهاب جريمة جنائية وطنية</u>

يعد الإرهاب في التشريعات الوطنية جريمة جنائية نظرا لما يتوافر فيها من أبعاد مختلفة من الجرائم، مثل القتل واستخدام المفرقعات، والاغتصاب، والسطو والسرقة والإتلاف. فهي علي هذا الأساس تعد جريمة فوقية تتميز بالعنف الذي وصفه البعض بأنه من خصائص الحرب أو النزاع المسلح. ويتطلب التكييف القانوني لجريمة الإرهاب تعريفا قانونيا للجريمة يحدد أركانها يتبناه المشرع وفقا لمبدأ شرعية الجرائم والعقوبات، مع الالتزام بمبادئ الضرورة والتناسب عند التجريم والعقاب بالأفعال التي يتضمنها هذا التعريف،. وتتميز هذه الجريمة بذاتية خاصة من الناحية القانونية نظرا إلى جسامتها وهو ما ينعكس بوجه خاص في تجريم مجرد تأسيس الجماعات الإجرامية ومختلف الأعمال التي تساعد علي وقوع الإرهاب ومن بينها التمويل.[2]

---

(1) تركي ضاهر "الارهاب العالمي :إرهاب الدول وعمليات الإرهاب " ،( دار الحسام ، بيروت ، ١٩٩٤)،ص ص ٢٠-٦٥.
(2) عبد العزيز مخيمر عبد الهادي "الإرهاب الدولي مع دراسة الاتفاقيات الدولية والقرارات الصادرة عن المنظمات الدولية "دار النهضة العربية ،القاهرة ، ١٩٨٦،ص ص ١٢٠-١٧٠ .

٢- : الإرهاب جريمة دولية،

وتعتبر جريمة الإرهاب من الجرائم الدولية إذا كانت مخالفة للقواعد الدولية التي تترتب عليها المسئولية الجنائية الشخصية، سواء تلك التي نصت عليها الاتفاقيات الدولية أو تضمنتها القواعد الدولية العرفية، ويتطلب ذلك توافر العناصر الآتية: الاول : ألا تقتصر حدود الإرهاب علي دولة بعينها وإنما يتجاوز الحدود الوطنية للدولة سواء فيما يتعلق بالمتهمين أو بالوسائل المستخدمة أو بنوع العنف المستخدم والثاني أن تتم الأعمال الإرهابية بدعم أو بتشجيع أو بموافقة الدولة التي يوجد فيها مرتكبو هذه الأعمال أو بدعم دولة أجنبية( المادة٢ من اتفاقية المعاقبة علي تمويل الإرهاب ومن قبيل ذلك استخدام بعض وسائل الإعلام لخدمة أهدافها ، والثالث بالمجتمع الدولي بأسره علي نحو يمكن اعتباره تهديدا لأمن هذا المجتمع، وكونه أصبح عدوا لمجتمع الدولة الوطنية والمجتمع الدولي، بل هو عدو أكثر ضراوة لأنه لا يقبل أي حل تفاوضي ولا يبغي سوي النصر مهما كان الثمن غاليا في فقد الأرواح والدمار الذي يحققه.

والعنصر الرابع أن تبلغ هذه الأعمال حدا كبيرا من الجسامة تبدو في أدواته التي تصل إلي حد استخدام التكنولوجيا الحديثة أو الوسائل العسكرية التقليدية واتساع نطاقها، كما إذا زاد عدد ضحاياه. وفي هذه الحالة لا ينظر إلي المجني عليهم كأفراد وإنما ينظر إلي الإنسانية كلها كمحل لهذا الاعتداءو إذا كان استيفاء هذه العناصر لازما لاعتبار الإرهاب تهديدا للأمن الدولي، فقد استتبع ذلك اعتباره في ذات الوقت جريمة دولية، باعتباره ماسا بالقيم التي يؤمن بها المجتمع الدولي، ويتنازع الإرهاب- كجريمة دولية- ثلاثة أنوع من الأوصاف القانونية وفقا للقانون الدولي؛ الأول بصفته مجرد جريمة دولية، والثاني كجريمة ضد الإنسانية، والثالث : جريمة حرب.[1]

٣- : الإرهاب نوع من النزاع المسلح،

أطلق هذا الوصف القانوني تحت تأثير قرار سياسي أمريكي رأي أن الإرهاب قد يكون نوعا من النزاع المسلح، ذا ما اتسع نطاقه وزاد تطوره علي نحو يطلق عليه الإرهاب الذي يشعل الحربTerrorismeguerrier وقد اتخذ هذا الإرهاب صورة العنف الجماعيcollective violence، فاشتبه بذلك مع الحرب وقد بدأ هذا التشبيه في الولايات المتحدة منذ وقع الصراع بين تنظيم القاعدة في منتصف التسعينيات والإدارة الأمريكية، ويلاحظ أن الحرب نزاع مسلح يحكمه القانون الدولي الذي يضع طرفيه أمام القانون علي قدم المساواة. فقد تمسكت الولايات المتحدة وإسرائيل لتبرير استخدام القوة ضد الهجمات الإرهابية علي المواطنين في الخارج، كما سبق استخدام القوة من جانب إسرائيل ضد بيروت للرد علي ما سمي بهجمات إرهابية سنة١٩٦٨ ضد إسرائيل، كما استخدمت القوة إسرائيل القوة ضد تونس في ١٩٨٥ .

(1) عبد العزيز مخيمر عبد الهادي "الإرهاب الدولي مع دراسة الاتفاقيات الدولية والقرارات الصادرة عن المنظمات الدولية ، مرجع سابق ذكرة ص ص ٢٣-٤٥

## المطلب الثالث :

## هجمات الفضاء الالكتروني إرهاب أم حرب

تعد الحرب ظاهرة اجتماعية قديمة صاحبت الإنسان منذ نشأته على الأرض، وعبرت عن طبيعته التي وإن كانت تميل إلى السلم، فهي تلجأ إلى الحرب من أجل حمايته والمحافظة عليه، وهناك تعريف للحرب مفاده أنها أحد أشكال العنف الذي يتميز أساسا بأنه منهجي ومنظم فيما يتعلق بالجماعات التي تقوم بها، وبالطرق التي تستعملها من أجل ذلك. فالحرب هي "صراع مسلح دامٍ بين الجماعات المنظمة" لتحقيق غرض سياسي أو اقتصادي أو غير ذلك من الأغراض، لذا فهي تمثل القتل المنظم ويلجأ إليها لتحقيق أطماع مادية تدعو إليها مصلحة الدولة، وهي كذلك إحدى وسائل العنف، تلجأ إليها الدول لحل ما يقوم بينها من نزاعات أو سعياً لتحقيق غاية أو مطمع سياسي أو قومي وتهدف الحرب لتحقيق مصلحة من مصالح الدولة وفي سبيل نفعها الذاتي، لذا اختلفت المفاهيم، ولكنها ترتكز على أن الحرب علاقة بين دولة وأخرى.

وتتنوع أسلحة الحرب وفق التطور التكنولوجي والمرحلة التاريخية التي يحدث بها الصراع فهناك نوعان من التطور: الاول في ادوات القتال وتنوعها من الصورايخ والدبابات والطائرات وهناك ايضا التطور النوعي في تلك الاسلحة بزيادة قدرتها التدميرية والقتالية، وظهرت الاسلحة النووية والتي استخدمت بالفعل في أغسطس ١٩٤٥ بضرب هيروشيما وناجازاكي في اليابان في نهاية الحرب العالمية الثانية، وتتميز تلك الاسلحة باحتكار عدد قليل من دول العالم لها .[1]

وهناك الاسلحة الكيميائية، وهي قائمة على استخدام العناصر الكيميائية التي تؤدي إلى الاختناق، والاحتراق، وتفسخ الجلد والأعصاب. وهناك أيضا الحرب البيولوجية القائمة على استخدام كائنات مجهرية مثل الجراثيم المعدية والفيروسات، الأمر الذي يؤدي لانتشار الأمراض الخطيرة والقاتلة. وتتعدى المخاطر والحروب والأسلحة ما سبق للأسلحة الإشعاعية وهي وسائل مبتكرة لنشر المواد الإشعاعية التي تسبب الموت أو الإصابة خلال التعرض للإشعاع المنبعث منها. وهناك الأسلحة السيبيرية او اسلحة الفضاء الالكتروني التي يتم توظيفها عبر الفضاء الالكتروني. cyber weapons وهي تطوير وسائل لتعطيل الكومبيوترات الأساسية الداعم للبنية التحتية الوطنية، وتبقى الأسلحة التقليدية البسيطة لتصبح أكثر خطورة وتقتل أعدادا كبيرة.

وأصبح يمثل الفضاء الإلكتروني بعدا خامسا للحرب والإرهاب إلى جانب الأبعاد الاربعه الأخرى التقليدية المتمثلة في البر والبحر والجو والفضاء الخارجي وصعوبة التمييز بين الاستخدام الإرهابي لتكنولوجيا المعلومات وبين من يستخدم تكنولوجيا المعلومات والاتصال كسلاح أو هدف للهجوم في الفضاء الإلكتروني. وهناك حرب وإرهاب وعنف وقصف لمواقع واسري ومقاومة وقصف لمنشآت مدنية وعسكرية كل ذلك يتم في الواقع الافتراضي مع الاختلاف في الخصائص

---

(1) أمل حمود- مترجم"، روبرت هندي وجوزيف رتبلات، " أوقفوا الحرب.. إزالة النزاع في العصر النووي"، شركة الحوار الثقافي، بيروت، الطبعة: الأولى، ٢٠٠٥، ص ص ١٥٠- ٣١٦ .

والأهداف وطبيعة الضحايا وشكل وطبيعة المواجهة ونطاقها [1]. و أصبح الإرهاب ظاهرة مميزة كونه يعكس اتجاهات أوسع في الحرب غير النظامية والتي بدأت مع نهاية الحرب الباردة حيث الصراعات الدينية والعرقية، ففي تلك الحالة من الصراع لا يدور فيه بين جيوش نظامية يمكن تطبيق اتفاقيات جنيف بخصوص الحرب عليها، فحتى لو أن للقوات النظامية دور فإنه يقتصر على وضع الاستراتيجيات والخطط، فمع وجود تلك الجرائم الإرهابية يصعب إمكانية تحميل أي شخص مسئوليتها حيث لا يمكن إثبات من يتحمل مسئولية هذه الإعمال، ومن هنا أصبحت الحرب غير النظامية منتشرة حول العالم وبدأ الإرهاب يدخل نطاق هذه الحروب غير النظامية خاصة إذا كان من يقومون بها أطراف من غير الدول، فالتهديد أصبح يأتي من الجماعات والمنظمات وحتى من أفراد.

وأصبحت الجيوش العسكرية في كافة أنحاء العالم تهتم بحرب المعلومات ودورها في حروب المستقبل، ووضع عدد من دول العالم إستراتيجية تهدف لتحقيق الأمن الالكتروني ضمن خططها الأمنية والدفاعية للمحافظة على مصالحها الاقتصادية والسياسية والعسكرية، وظهرت هناك مناورات يتم إجراؤها للتدريب على مثل هذا النوع الجديد من الصراع وكيف يمكن مواجهته والاستعداد له، ففي الصين هناك تدريب ميداني للجيش الصيني يستخدم تقنيات متطورة ويمكن توقع استخدامها للفضاء الالكتروني لمهاجمة أعدائها في حالة أي قتال ينشب في المستقبل. ويصبح هناك إمكانية استخدام الشعب بأكمله كشريك في الحرب مع العسكريين[2]

ويتم مفهوم إدارة الحرب الشعبية من خلال استخدام المدنيين للكمبيوتر الشخصي، فإن هؤلاء الذين يديرون الحرب ليسوا كلهم بالضرورة من العسكريين، وأن أي شخص مدني لديه أساسيات معرفة الكمبيوتر والإنترنت يمكن أن يصبح محاربا من خلال شبكات الإنترنت، كما أضاف اصطلاحاً جديداً اسمه "دبابات الفكر" Think tanks المكونة من خبراء غير حكوميين مختارين من الصفوة العلمية، يعملون على أجهزة الكمبيوتر الشخصي، ويشتركون في عملية صنع القرار على المستوى الأعلى.

ولن تكون التعبئة العسكرية كما يرى "(جوانج) مقصورة على العسكريين الشباب، ولكن سوف يكون أول من يتم تعبئتهم هم هؤلاء المدنيين الذين يجلسون على مقاعدهم خلف الفضاء الإلكتروني ويسبحون من خلاله، وظهر الارتباط بين تكنولوجيا الاتصال والمعلومات والحرب بكافة أنواعها لتظهر في شكل تطوير للفكر النمطي في شن الحرب ووسائلها فيما يطلق علية الثورة في الشؤون العسكرية وحروب المستقبل.[3] وأصبحت حرب المعلومات واستخدامها كأداة

---

(1) في بداية الحرب العالمية الاولى في اغسطس ١٩١٤ قامت شركة تليكونيا البريطانية telconia بقطع الكابلات البحرية الالمانية بما دفع الالمان لدخول الحرب ، كما دفع قيام شركة Zimmerman للتلغراف بالتدخل في عمل الكابل البحري من المانيا الى المكسيك الامر الذي دفع ايضا الولايات المتحدة الى دخول الحرب العالمية الاولى ، كما قامت الدول باستخدام موجات الراديو في كل من حالة السلم والحرب طيلة ٦٠ عاما ماضية بدا من قيام النمسا بمنع البث الاذاعي القادم من المانيا النازية في ١٩٣٤.

(2) قدّم أحد المفكرين العسكريين الصينيين واسمه (شان وي جوانج) عام ١٩٨٥م في دراسة شاملة، تعدّ أول أوراق عسكرية صينية ويرز في هذه الدراسة اصطلاح علمي جديد وهو (حرب الغرف المغلقة) أو (حرب المنازل) home battle Take،

(3) جلال المنزلاوي " ماذا يدور خلف السور العظيم؟ "، مجلة كلية الملك خالد العسكرية، العدد (٧٨) ٠١/٠٩/ ٢٠٠٤

للإرهاب تعكس اتجاهات أوسع في الحرب غير النظامية والتي بدأت مع نهاية الحرب الباردة حيث الصراعات الدينية والعرقية، ففي تلك الحالة من الصراع لا يدور بين جيوش نظامية يمكن تطبيق اتفاقيات جنيف بخصوص الحرب عليها، فحتى لو للقوات النظامية دور فانه يقتصر على وضع الاستراتيجيات والخطط، فمع وجود تلك الجرائم الإرهابية يصعب إمكانية تحميل أي شخص مسئوليتها حيث لا يمكن إثبات من يتحمل مسئولية هذه الأعمال.

وأصبحت الحرب غير النظامية منتشرة حول العالم ويبدا الإرهاب يدخل نطاق هذه الحروب غير النظامية خاصة إذا كان من يقومون بها أطراف من غير الدول. و يأتي التهديد من الجماعات والمنظمات وحتى من أفراد، ويمكن أن تنتشر حرب المعلومات بسرعة عالية، ويمكن أن يشنّها أي شخص على اتّصال بالإنترنت ويستطيع تتبع التعليمات البسيطة، المعروضة أمامه على شاشة الكمبيوتر. وربما يؤدي منحى تزايد نقاط الضعف - مقروناً بمدى ملاءمة الهجوم وقدرته على حرمان الخصم من معلومات عن المهاجم - إلى اندلاع حرب المعلومات بمشاركة أفراد ومجتمعات وشركات ودول، وربما تحالفات. وسيكون تأثيرها هائلاً.[1] وأصبح مفهوم الهجوم يختلف عن شكله التقليدي حيث أصبح جهازاً يستخدم لمهاجمة أجهزة أخرى ،وإمكانية إصابة الهدف بسهولة عن طريق هجوم الفضاء الإلكتروني وخاصة إصابة مراكز القيادة والسيطرة الخاصة بالبنية التحتية الحرجة كمحطات الطاقة بالإضافة إلى أنظمة التسلح وفي العمليات الحربية العدائية . وساعد انتشار تكنولوجيا المعلومات وعلاقتها المباشرة بالجوانب المدنية والعسكرية إلى اتساع ميدان الحرب لتمتد إلى حرب وهجمات متعددة الأبعاد والتي تشمل الأرض والبحر والمجال الجوي والفضاء الخارجي والالكتروني وتم وصف الأخير بالمجال المعلوماتي، .حيث تكون الحرب موجهه معلوماتيا ،وجاءت تلك التغييرات لتنعكس على مفهوم الحرب التقليدية بإضافة التكنولوجيا بكافة أنواعها في المجال الحربي حيث أضافت عدة تغييرات على مفهوم الحرب والإرهاب حيث يعتبر الأخير شكلا مختلفاً عن الحرب و حتى عن حرب العصابات لأنها تكون موجهة فقط إلى الجيش النظامي وترتبط بتحقيق أهداف محلية كالاستقلال الذاتي أو مطالب فئوية، وتمتلك القدرة على التطور وفقا لتحقيق أهدافها السياسية ومن ثم فهي قابلة للانتهاء بتحقيق مطالبها. وهناك صعوبة التمييز بين الخطوط الفاصلة بين عمليات الدفاع أو عمليات الهجوم، وهنا ينبع الخلط بين العمليات والأهداف والإستراتيجية والتكتيك. ويصبح الإرهاب سواء أقامت به دول أو أفراد أو جماعات يتميز بقدرته على التلون والتشكل وفق مقتضيات العصر بما يتلاءم مع تحقيق الهدف من ورائه، وجاء الإنترنت كإحدى الوسائل التكنولوجية الحديثة التي يمكن استخدامها وبكفاءة وجاءت الجماعات بكافه أشكالها وأطيافها السياسية من يسارية ويمينية وراديكالية وأصولية وفوضوية وغيرها من الأشكال باعتبارها الأضعف، ولتمارس هذا النوع من الإرهاب الجديد عبر الفضاء الإلكتروني إما ببث الكراهية الدينية والتحريض أو المساعدة في العمل الإرهابي التقليدي أو شن حرب الكترونية خالصة.

---

[1] David J Lonsdale,. **The Nature of War in the Information Age**: Clausewitzian Future. New York, Frank Cass, 2004. p. 269.

## المبحث الثاني :
## ماهية مفهوم الإرهاب الالكتروني وإشكالياته
## والمفاهيم ذات الصلة

**يتعرض هذا المبحث الى محاولة التاصيل المفاهيمي للارهاب الالكتروني والتعرض لاشكاليات تحديد مفهوم واضح لة وذلك وفقا لخصائصه المتنوعه وتداخل طبيعة ذلك المفهوم مع غيرة من المفاهيم المترابطة به ويتم ذلك من خلال تناول المطلب الأول: ماهية وإشكاليات مفهوم الإرهاب الالكتروني والمطلب الثاني: خصائص الإرهاب الالكتروني والمطلب الثالث: آليات وأدوات الإرهاب الالكتروني والفاعلون وذلك على النحو التالي :**

### المطلب الأول:
### مفهوم الإرهاب الالكتروني: الماهية والاشكاليات

مع نمو شبكة الإنترنت في كل من حجمها ووظيفتها منذ السبعينات إلي الوقت الحاضر، شهد العالم تغييرا هائلا في كل من طبيعة التهديدات ومستوى النشاط الهجومي الموجه ضد الإنترنت - الأنظمة المتصلة به، ففي أثناء العقد الأخير دخل الإنترنت إلي قطاعات واسعة من الخدمات الحكومية والصناعة والاتصالات والمعاملات المالية والتجارية ووسائط الإعلام المختلفة، وأصبح الإنترنت وسيلة فعاله من حيث التكلفة وسرعة الانتشار، ومع زيادة الاعتماد المتزايد عليه زادت بالمقابل درجة التهديدات المحتملة التي يمكن أن تعترض تلك الشبكة وخاصة من الإرهاب الذي يمكن أن يوجهه لتلك الأنظمة الحديثة التي أصبحت جزءا لا يتجزأ من النمط الحديث للحياة المعاصرة وخاصة ما يتعلق بالبنية التحتية الحيوية للمعلومات.

فالإرهاب المادي هو الاستخدام غير المشروع للقوة أو العنف ضد الأشخاص أو الممتلكات لترويع أو إجبار الحكومات أو الناس العاديين أو أي جزء منهم من أجل تحقيق أهداف اجتماعية أو سياسية. ومع بداية موجة الانتشار التكنولوجي عالميا وتصاعد مستوى الاهتمام بقطاع تكنولوجيا الاتصال والمعلومات كمدخل هام لتحقيق نمو اقتصادي سريع، جاء ظهور التهديد بالاستخدام السلبي لتلك المعطيات التكنولوجية من قبل مهددات كثيرة مثل إمكانية استخدام تلك المعطيات في التحضير أو القيام أو التنسيق أو التعبئة أو الحشد للعمل الإرهابي، وظهرت مسميات تعبر في مجملها عن انشطة غير سلمية للفضاء الالكتروني على نحو يؤثر في طبيعته ودوره ويؤثر بالتالي على اهميته الاستراتجية في النظام الدولي، ومن ضمن تلك المسميات واشهرها مفهوم "الإرهاب الإلكتروني".

وجاء هذا المفهوم مقترنا في بداية ظهوره بنمط من الدعاية المضللة مع غموض المفهوم وعدم وضوحه ، وأصبح تحديد ماهية "الإرهاب الإلكتروني" بكل مفرداته المقابلة والمترادفة والمتداخلة معه جزءا من المشكلة، وظهرت على نطاق واسع تعريفات مختلفة تدور حول 'الاستخدام الإرهابي للتكنولوجيا'"، و أصبحت هناك علاقة وثيقة الصلة بين ظاهرة الإرهاب الدولي الجديدة وتكنولوجيا الاتصال والمعلومات التي تعد بُعدا هاما من أبعاد العولمة. ولم يعد الفعل العنيف الذي يأتي في صورة إرهاب أو حرب حصيلة اجتهاد وفعل مجموعة أفراد محدودة العدد وقليلة التاثير، ولم يعد فعل الحرب يأتي من قبل جيش

نظامي في مواجهة جيش نظامي في دولة أخرى، واصبحت الحرب تتجه الى ان تاتي في شكل مجموعه اعمال ارهابية، وأصبح العمل الإرهابي يأتي من منظمات صغيرة متناثرة هنا وهناك لديها القدرة على ان تقوم بعملا منظما ومؤسساً على آليات التجنيد والتعبئة والاستفادة من وسائل الإعلام والاتصال الحديثة.

وباتت المنظمات المستخدمة للعنف من أجل أغراض سياسية أو بدوافع دينية، حتى في أكثر صورها محلية، غير بعيدة عن توظيف الفضاء الإلكتروني الذي يشمل تكنولوجيا الاتصال والمعلومات و هواتف محمولة وحاسبات آلية وعبر شبكة الإنترنت، واتاحت تلك الاليات إمكانية الاستفادة منها في القيام بأنشطة المضاربة في البورصات العالمية وإجراء التحويلات المالية والتنسيق وجمع المعلومات، وظهر ذلك في استخدام الجريمة المنظمة الدولية وتجارة المخدرات والجماعات الارهابية، كما أن شكل الإرهاب في العصر الحديث قد اتخذ من العولمة وما اتاحته من وسائل في ذات الوقت وسيلة للهجوم وتعبيراً عن استخدام القوة في العلاقات الدولية، وظهر الإرهاب الإلكتروني وفقا لطبيعته الفيزيائية إرهابا معلوماتيا وانعاكساً في الوقت نفسه لثورة المعلومات في العصر الحديث.

وقد كانت بداية استخدام هذه الكلمة cyber terrorism في فترة الثمانينات في دراسة "باري كولن" Barry Collin والتي خلص فيها إلي صعوبة تعريف ظاهرة الإرهاب التكنولوجي بدقة، ناهيك عن الأساليب والحلول المطلوبة لمواجهته وكذلك تحديد دور الكمبيوتر والإنترنت في العمل الإرهابي.(1)

وفي عام ١٩٨٠ كان يشير ذلك المصطلح إلي تلك الهجمات التي يستخدم فيها الكمبيوتر ضد اقتصاد وحكومة الولايات المتحدة، ثم اتسع هذا المفهوم مع بداية التسعينات التي شهدت حدوث نمو متزايداً في انتشار ادوات تكنولوجيا الاتصال والمعلومات دولياً في اطار ظهور مجتمع المعلومات العالمي، وظهرت العديد من الدراسات التي تناولت المخاطر المحتملة التي تواجه الدول الغربية خاصة الولايات المتحدة في اعتمادها الكبير على التكنولوجيا وأجهزة الكمبيوتر، وفي تلك الفترة أي في بداية التسعينات صدر تقريرعن الأكاديمية الوطنية الأمريكية للعلوم عن أمن الكمبيوتر جاء فيه "نحن بصدد مخاطر متزايدة بسبب اعتماد الولايات المتحدة على أجهزة الكمبيوتر حيث غدا بإمكان الإرهابيين أحداث تدمير أكبر بالاعتماد على لوحة المفاتيح أكثر من استخدام القنبلة، وقد يتسبب ذلك في بيرل هاربور الكتروني جديداً"، وظهر عدد من التعريفات التي تركز على ناحية ما من الخطر وتتجاهل نواحي أخرى.

وهناك من التعريفات ما يركز على أوجه التشابه مع الإرهاب بشكله التقليدي وهناك تعريفات فضفاضة والتي انطلقت بهدف الابتعاد عما قد يكون له أثر سلبي على التطور التكنولوجي وطبيعة المنافسة بين الشركات العاملة في قطاع تكنولوجيا الاتصال والمعلومات، ومن ثم فإنها عملت على تشجيع الانتشار التكنولوجي والاتصال بالإنترنت واقتناء خدماتها والاهتمام بالجانب الإعلامي في حين جاء الاهتمام بالأمن متأخرا حين ظهر الاستخدام السيئ لتلك الأدوات، وأصبح هناك عجز عن تقديم

---

(1) Kathryn Kerr," **Putting cyberterrorism into context**", Auscert,24 October 2003,
للمزيد يمكن الاطلاع على تلك الدراسة على الموقع التالي، ( اخر زيارة ٢٠-٤-٢٠٠٨)
(http://www.auscert.org.au/render.html?cid=2997&it=3552)

التفسير والفهم الشامل والمعنى الجامع المانع لما يطلق علية الإرهاب الإلكتروني. وأعقب ذلك اجتهادات لوضع تعريف محدد لما يمكن إن يطلق علية "الإرهاب الإلكتروني " ومحاولة تحديد بعض الاستخدامات الخاطئة للمفهوم، بشكل يمكن إن نقبل طريقة استخدام المفهوم وطرق التمييز بين ما يمكن إن يعترض الشبكات من خطر الهجمات التي يمكن إن توصف بالإرهابية إي يكمن ورائها هدف سياسي وبين غيرها من الأخطار التي تهدد أيضا امن الفضاء الإلكتروني.(1)

حيث إن الإرهاب الإلكتروني هو استخدام الفضاء الالكتروني كأداة لإلحاق الضرر أو تعطيل البنية التحتية القومية الحرجة (كالطاقة، المواصلات، وعمليات الحكومة، ويدخل الإرهاب الإلكتروني ضمن الأنواع الأخرى التي تصب في اتجاه هدف سياسي واحد والتي قد تتحالف مع الجريمة أو تكون إحدى أدواتها، ويأتي من نتاج التفاعل فيما بين العالم المادي والافتراضي، فالعالم المادي هو المادة والطاقة الموجودة حيث تعيش وتعمل.... ، أما العالم الافتراضي فهو الرمز القائم حيث تعمل برامج الكمبيوتر وتتحرك المعلومات بصورة رقمية ومجازية، وعلى الرغم من تباينهما إلا أنهما يتفاعلان لحين حدوث التقارب بينهما ليشكلا عرية الإرهاب الإلكتروني.(2)

والتي تأتي في صور عمليات تخريب توجه للشبكات وقواعد المعلومات لدى الطرف الخصم، بهدف إرباكه وتدمير قدراته في الحصول على المعلومات أو توظيفها في عملية المواجهة، أو منعه من ميزة الوصول إلى أعضائه أو المتعاطفين معه. ويظهر ذلك في تدمير مواقع الطرف الخصم الموجودة على الشبكة الدولية للمعلومات " الإنترنت". أو اختراق شبكات المعلومات الرسمية للوزارات والإدارات الحكومية والمصارف بغية تخريبها أو الحصول منها على الأسرار وتدمير المواقع على الإنترنت.فإذا كان الإرهاب يعني في ابسط تعريفاته " الاستخدام السياسي للعنف ضد المدنيين " لكن ثمة اتجاه هام يوجد توافق نسبي بشأنه يستند على إمكانية وضع معايير معينة أو " روابط" يمكن من خلالها تحديد المقصود بالعمل الإرهابي، كأساس للتعريف، ولتطبيق ذلك على الإرهاب الإلكتروني يكون هناك ثمة عناصر مشابهه يمكن ملاحظتها في التعريفات التالية:

١. قطبقاً لتعريف " وكالة المخابرات المركزية الأمريكية ":"الإرهاب الإلكتروني هو أي هجوم تحضيري ذي دوافع سياسية موجهه ضد نظم معلومات الكمبيوتر، وبرامجه، والبيانات والمعلومات والتي تتتج من عنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين "

٢. وتعريف مركز حماية" البنية التحتية القومية الأمريكية ":الارهاب الالكتروني على أنه " عمل إجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان، وذلك بهدف التأثير على الحكومة أو السكان لخدمة أجندة سياسية أو اجتماعية أو ايدولوجيه "

(1) Library of Congress. Congressional Research Service. **Information Operations and Cyber war: Capabilities and Related Policy Issues,** by Clay Wilson. Washington, CRS, September 14, 2006.pp 9-18.
(2) Dan Verton," **Black Ice: The Invisible Threat of Cyber-Terrorism**. New York, McGraw-Hill/Osborne, 2003.pp 180 – 273.

٣. أما تعريف " دينيج دوروثي " Denning " "(١) فتعرفه على انه "هجمات غير قانونية وتهديدات بالهجوم ضد الحاسبات والشبكات والمعلومات المخزنة وذلك لكي توظف لتخويف أو إجبار حكومة أو شعبها بهدف تعزيز أهداف سياسية أو اجتماعية ، ولكي يكون إرهاباً يجب إن ينتج عنه عنف تجاه الأفراد أو الممتلكات أو على الأقل التسبب بضرر ينتج عنه توليد الخوف "(٢)

٤. واما "جيمس أ. لويس ": مركز الدراسات الإستراتيجية والدولية (٢٠٠٢)فيعرفه على انه "استخدم أدوات شبكات الكمبيوتر لتعطيل البنية التحتية القومية (مثل الطاقة، المواصلات، عمليات الحكومة ) أو أكراه أو ترهيب الحكومة أو السكان المدنيين "(3).

٥. وتطرح وزارة الدفاع الأمريكية للارهاب الالكتروني تعريفاً مفاده " انه عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنه عنف وتدمير أو بث الخوف تجاه تلقي الخدمات بما يسبب الارتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينه "(٤).

ويمكن القول أن هناك تعريفين هما (٢&٤) حددا إن نظم الكمبيوتر أو وسائل الاتصالات يمكن استخدامها في هجمات الإرهابيين عبر الفضاء الإلكتروني، أما التعريفان الآخران (١"&٣) حدد فقط الكمبيوتر ونظم المعلومات كأهداف لهجمات الإرهابيين، ومن ثم فان هناك حاجة لأن يتم تضمين هذين العنصرين في تعريف واحد، ففي إثناء تعرض نظم المعلومات للهجوم بأي عدد من الوسائل كطرق تقليدية كالقنابل أو إشعال الحرائق وغيرها. فان ذلك الفعل يمكن أن يدخل ضمن تعريف "الإرهاب الإلكتروني"، فالمهاجم يمكن إن يستخدم نظم المعلومات أو الوسائل الالكترونية الأخرى لكي يتمكن من شن الهجوم. كما انه يمكن إن يتم استخدام الأدوات العسكرية التقليدية من اجل قصف مراكز الاتصال وشبكات الإنترنت أو حتى الأقمار الصناعية.

وفي حالات كثيرة يتم استخدام كل من مفهوم "هجوم الفضاء الإلكتروني " و"الإرهاب عبر الإنترنت " بنفس المعنى وهذا ما قد يسبب سوء فهم في معنى الهجوم الالكتروني عبر استخدام الفضاء الإلكتروني بمعناه الشامل وخطر الإرهاب عبر الإنترنت بالتحديد، هذه التعريفات يمكن إن نستخلص منها انه لكي يكون هناك ما يمكن إن نطلق علية إرهاباً يجب أن تتوافر ثلاثة عناصر والتي يمكن من خلالها التمييز بين هجوم السيبري الإرهابي من هجوم الإنترنت العادي، وقد لاحظت " دينيج " إن هجمات الفضاء الإلكتروني ذات الدافع السياسي والتي يمكن إن تؤدي إلى الموت أو التسبب في جرحى أو تفجيرات أو خسارة اقتصادية تمثل نماذج للإرهاب الالكتروني، فالهجمات الخطيرة ضد البني الأساسية

---

(1) Sarah Gordon & Richard Ford ,"**Cyber terrorism**" ,Symantec cooperation (the world leader in internet security technology ) ,USA,2003 .
(2) Denning, D "Cyberterrorism" ,August 24, 2000.
( http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc)
(3) Lewis, J.A., **Assessing the risk of cyber terrorism, cyber war and other cyber threats**, Center for Strategic and International Studies, (2002)( http://www.csis.org/tech/0211_lewis.pdf)
(4) **Information Warfare and the Air Force: Wave of the Future? Current Fad?"**, RAND, March 1996.

الحيوية يمكن أن تكون أعمال الإرهاب عبر الإنترنت، اعتمادا على أثرها. من حيث تعطيلها للخدمات أو خسارتها الاقتصادية [1]

وركز التعريف الرابع فقط على إصابة البنية التحتية وذلك دون الإشارة إلى الدافع السياسي من وراء تلك الهجمات.[2] وهناك تنوع واضح في تعريف مفهوم الإرهاب الإلكتروني وفي الواقع إن هناك صعوبات في إيجاد تعريف واضح ومكتمل للإرهاب الالكتروني بسبب إن ما تم تناوله جاء بشكل درامي وتخيلي و أكثر حساسية ولم يتم تناوله بشكل عملي جيد ، ويرجع ذلك أيضا إلى شيوع استخدام أجهزة الحاسب وتنوع الأهداف والوسائل والأشخاص ، والاهم من ذلك كله انه على المستوى الدولي لم يتم إلى الآن الاتفاق حول مفهوم واضح للإرهاب .

ويمكن ملاحظة في كل تعريفات الإرهاب الإلكتروني أن هناك عناصر مشتركة مثل الأفراد أو المجموعات أو المواقع مادية أو افتراضية الكترونية طرق التنفيذ والأهداف والأدوات والدوافع، وقد انعكس ذلك التعدد على طبيعة الإرهاب وتعريفة بل امتد ذلك التعدد إلى المستوى الاصطلاحي للكلمة، وهناك تداخل واضح بين عدد من المفردات [3] لتعبر عن إستراتيجيات عسكرية وسياسية و شكل جديد من الحرب والإرهاب .

ويمكن التفريق بين حرب المعلومات والإرهاب الإلكتروني حيث تنقسم حرب المعلومات لنوعين نمط هجومي ونمط دفاعي، فالهجومي تقوم به في الغالب الدولة وأجهزة استخباراتها لما تمتلكه من إمكانيات ضخمة تؤهلها للقيام بها، وتستخدم حرب المعلومات الهجومية لأهداف سياسية وعسكرية أو لمجرد الإثارة أو لتحقيق أهداف إجرامية، ويستحوذ المهاجم على المعلوماتية ونظمها، ويقوم بالتجسس وسرقة البرامج الكمبيوترية، وتخريب أو تعطيل نظم المعلوماتية. أما الحرب الدفاعية فتعمل على الحد والوقاية من أعمال التخريب التي قد تتعرض لها، وتختلف الوسائل الدفاعية باختلاف أدوات التخريب والمعلوماتية وطبيعة الأضرارالتي قد تحدثها [4]

وتستخدم الحرب المعلوماتية لتحقيق أهداف إستراتيجية والتي قد تستخدم لتحقيق أهداف قومية عن طريق التأثير أو السيطرة على كل العناصر ( السياسية والاقتصادية والعسكرية والمعلوماتية )، أما على المستوى العملياتي الميداني فإنها تستخدم للتأثير على شبكات الاتصالات والدعم اللوجستي والقيادة والسيطرة وكل الأنشطة والإمكانيات التي يمكن إن تستخدم، إما على المستوى التكتيكي فهي تهدف إلى التأثير على المعلومات وأنظمة البيانات التي تعتمد عليها بشكل مباشر والتي ترتبط

---

(1) D.E. Denning, Cyberterrorism,op.cit

(2) ________., (**Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy**, 1999( http://www.nautilus.org/info-policy/workshop/papers/denning.html)

(3) يمكن التعبير عنها بعد استبدالها مثلا بثلاث مفردات (Cyber أو Computer أو Information ) بعدد ضخم من الكلمات المترادفة ذات الطبيعة التركيبية في اللغة الإنجليزية Cyber crime, cyber war, info war, net war cyber terrorism cyber harassment ,virtual warfare, digital terrorism, cyber tactics, cyber break-ins

(4) Lech J. Janczewski and Andrew M. Colarik,(eds)," **Cyber Warfare and Cyber Terrorism**" ,. Hershey, PA, Information Science Reference, 2008. p. 532.

بالعمليات العسكرية.[1] وهنا يبرز تداخل ما بين الحرب المعلوماتية والإرهاب الإلكتروني في شكل استخدام للقوة، وهناك العديد من الأوصاف الأخرى للإرهاب الجديد، وتثور هنا قضية من يضع التعريف ومن يتخذ الإجراءات المضادة، فعلى الرغم من أن الأدبيات منذ فترة كبيرة حوت تعريفا واضحا لما سمي بالإرهاب الدولي، إلا إن ذلك المفهوم قد لقي في الوقت المعاصر صعوبات في تحديد تعريف له بسبب كون تلك القضية أصبحت مسيسة أكثر من السابق. إلى جانب تغير أثر استخدام تكنولوجيا المعلومات والاتصال على طبيعة الإرهاب نفسه، وركزت كافة تعريفات الإرهاب على انه عمل مادي يقع في الحيز الواقعي سواء في الوسائل أو النتائج، وركزت كذلك تلك التعريفات على إن الدولة هي المقصودة بالعمل الإرهابي سواء أكان من طرف الجماعات الإرهابية أو بدعم من طرف دولة، وان العمل الإرهابي نفسه هو عمل عسكري محدود بهدف إلحاق الأذى بالدولة في حين إن الإرهاب الجديد ارتبط بفكرة الإرهاب الثقافي نتيجة العولمة والثورة التكنولوجية.

وقد ركزت التعريفات القديمة للإرهاب على انه يعتمد على وسائل عنيفة بالضرورة في إحداث هذه الحالة من الرعب، وأنة يكتسب صفته الدولية من كونه يمس عنصراً أو أكثر من دولة أو شخص أو مؤسسه تحت الحماية الدولية.أما الآن فلم يعد يكتسب الإرهاب صفته الدولية بذلك فالإرهاب قد يوجه إلى دولة ويعناصر محلية ويخسائر تقع في نطاق الدولة ولكنها تكتسب طابعها الدولي مثل أحداث الحادي عشر من سبتمبر٢٠٠١ حيث تأثر الاقتصاد العالمي فور وقوعها وما نتج عنه من تغييرات بالاتجاة إلى الحرب الوقائية.

ومع كل الاجتهادات التي حاولت إيجاد تعريف محدد لمفهوم الإرهاب الإلكتروني فانه قد يعني "العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد عبر الفضاء الإلكتروني أو أن يكون هدفا لذلك العدوان بما يؤثر على الاستخدام السلمي له "،

اما عن تعريفة اجرائيا فانه قد يعني " نشاط أو هجوم متعمد ذو دوافع سياسية بغرض التأثير علي القرارات الحكومية أو الرأي العام باستخدام الفضاء الإلكتروني كعامل مساعد ووسيط في عملية التنفيذ للعمل الإرهابي أو الحربي من خلال هجمات مباشره بالقوة المسلحة على مقدرات البنية التحتية للمعلومات، أو من خلال ما يعد تأثيرا معنويا ونفسيا من خلال التحريض علي بث الكراهية الدينية وحرب الأفكار، أو أن يتم في صورة رقمية من خلال استخدام آليات الأسلحة الالكترونية الجديدة في معارك تدور رحاها في الفضاء الإلكتروني والتي قد يقتصر تأثيرها علي بعدها الرقمي أوقد تتعدي لإصابة أهداف مادية تتعلق بالبنية التحتية الحيوية "[2] .

و يأتي الإرهاب الإلكتروني في صورة القيام بهجوم طبيعي عن طريق استخدام الأسلحة التقليدية كالقصف المباشر بالقذائف في عملية مهاجمه كابلات الاتصال ونقاط الإنترنت الرئيسية والأجهزة أو

---

(1) Michael N. Schmitt, **Wired warfare: Computer network attack and jus in bello** , RICR Juin IRRC ,Vol. 84 No 846, June 2002.

(2) عادل عبد الصادق، " هل يمثل الإرهاب الإلكتروني شكلاً جديدا من أشكال الصراع الدولي "، ملف الاهرام الإستراتيجي،مركز الدراسات السياسية والاستراتيجية ،جريدة الاهرام ، العدد ١٥٦ ديسمبر ٢٠٠٧.

عن طريق القيام بهجوم عن طريق استخدام الطاقة الكهرومغناطيسية واستخدامها كقوة عن طريق القيام بهجوم Electronic Attack ضد أجهزة الكمبيوتر أو البيانات بداخلها بما يؤثر على عملها .

وتستخدم هجمات الفضاء الإلكتروني Cyber attack أو هجوم شبكات الكمبيوتر Computer Network Attackعن طريق استخدام أسلحة الفضاء الإلكتروني بما يؤثر على الامن والطابع المدني له ، وقد أحدثت الحرب التي تم شنها ما بين جورجيا وروسيا ٢٠٠٨ ، وما بين روسيا واستونيا عام ٢٠٠٧ تداخلا واضحا ما بين الاستخدام الإجرامي للفضاء الالكتروني والإرهابي والحربي حيث تلاشت الحدود الفاصلة ما بين القدرة على التمييز بين الإرهاب والحرب والجريمة.(1)

وقد يأخذ الإرهاب الإلكتروني طابعاً غير عنيف من خلال التحريض على الاعتداء أو القتل أو بث العنصرية والتأثير على الرأي العام والجمهور والقيام بحرب نفسية أو العمل على التأثير الاقتصادي بما يكون له تأثير على الاستقرار السياسي بما تخلفه هجمات الإرهاب الإلكتروني بكافة أنواعها من التأثير على الاقتصاد الدولي سواء من خلال عمليات التجارة الالكترونية أو تقديم الخدمات الحكومية أو سرقة أسرار صناعية أو أداء المؤسسات المالية الدولية والبورصات التي يحركها طلبات الشراء والبيع والتي تتأثر بما يتم تداوله من أخبار أو شائعات تضر بالمصالح القومية ، حيث أن الفضاء الإلكتروني قد عمل على تلاشي الحدود الدولية أو سلطة رقابة الدولة على إعلامها بظهور إعلام الكتروني يتميز برخص التكلفة وسرعة الانتشار حيث يبدو الفضاء الإلكتروني كوسيلة إعلام دولية .

وفيما يتعلق بالبعد العسكري للإرهاب الإلكتروني يمكن أن ياتي باستخدام نظم المعلومات من اجل التسبب بإلحاق أضرار في شكلين الاول بشن هجمات شبكات الكمبيوتر Computer Network Attack (CNA) أو في عمليات الدفاع عن طريق شبكات الكمبيوتر ( Computer Network Operations CNO)، وتأتي الثانية عن طريق جمع المعلومات والاستخبارات واستغلال أنظمة العدو من اجل دعم المتطلبات الاستخباراتية أو جمع المعلومات التي تسهل عمليات هجوم شبكات الكمبيوتر، و يمكن أن يستخدمها الإرهابيون والمجرمون سواء دعمتهم دولة أم لا عن طريق الكمبيوتر وجمع المعلومات حول الأهداف المتحركة والثابتة أو دعم عمليات المعلومات والتي قد تؤدي إلى المساعدة في تنفيذ أهدافهم، بينما يتم استخدام هجمات شبكات الكمبيوتر ضد شبكات العدو والتسبب في هجوم إنكار الخدمة أو العبث في نظمها وطريق عملها بما يؤدي إلى إفسادها وتعطيلها.

ويبدا خطر الإرهاب الإلكتروني من آليات منفصلة لتشكل فيما بعد خطرا استراتيجيا كبيرا، خاصة إذا ما تم التنسيق مع خطط تقليدية تقوم بها دول في شكل أجهزة استخبارات أو جماعات إرهابية حيث ترتفع في مستويات التنسيق ليتم استغلال تقنيات حرب المعلومات لإصابة المرافق الحيوية، ومن ثم فان الأهداف التي قد تكون عرضه للتهديد مجتمعه أو فرادى ذات الصفة المادية المباشرة هي تخزين المعلومات، وعملية إدخال المعلومات، وإرسال واستقبال الرسائل، و التحكم في الأجهزة

---

(1) Clay Wilson," **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress**",Congressional Research Service, January 29, 2008 (http://italy.usembassy.gov/pdf/other/RL32114.pdf)

والتصميم وباستهداف البنية التحتية القومية للمعلومات وخصوصا في مجال التكنولوجيا التي تجمع قطاعات الكهرباء والاتصالات والكمبيوتر وهي من ركائز الأمن القومي الجديد، والتي تكون معرضة لتهديدات الحرب الرقمية، وهي تقوم على أساس المصادر التي يعتمد عليها من يريد القيام بهجوم رقمي متوافرة ومنتشرة بين عامة الناس وتتألف من جهاز كمبيوتر ونقطة اتصال بالإنترنت وبذلك تعددت مصادر التهديد ومكان انطلاق الحرب(1).

## المطلب الثاني:
## خصائص الإرهاب الالكتروني

أحدثت الثورة التكنولوجية في الاتصالات والمعلومات ثورة فكريه في مفاهيم الحرب والعدوان وفي مضامين القانون الدولي بل وفي الفاعلين وفي الوسائل أيضا، فلم يعد هناك مجال لإعلان حالة الحرب بين الدول أو بين الجماعات والدول حيث الاعتماد على الضربات الاستباقيه، فالحرب لم تعد بالضرورة قصف مواقع عسكريه مادية بل شملت الحرب الدخول لأنظمة المعلومات وتدميرها أو التأثير في كيفية عملها مما يكون له اكبر الأثر في ظل الاعتماد المتزايد للدول على التكنولوجيا في الاقتصاد والسياسة وفي شتى مجالات الحياة.

وقد ازدادت طبيعة التفاعلات بين البشر في كافة أرجاء العالم وأصبحت تلك التفاعلات معقدة لتصبح عملية التعاطف والتجنيد على مستوى العالم مفتوحة بوصول أفكار تلك الجماعات إليها، ومن ثم دخل عنصر الحلفاء المفترضين حيث لا يجمعهم سوى الاتفاق حول أهداف وليس بالضرورة استراتيجيات معينة لتصبح جماعات أكثر لامركزية في التنفيذ ومركزيه في الأفكار، وعمل ذلك على التأثير على الإرهاب التقليدي بينما أنتج الفضاء الالكتروني عولمة للبيئات المحلية وزيادة الترابط بين ما يحدث محليا وعالميا كتأثير أحداث ١١ سيتمر٢٠٠١ على الاقتصاد العالمي، ففي الإرهاب التقليدي يتم فيه استخدام أو التهديد باستخدام العنف ولكن أصبح هناك شكل من القوة والعنف والعدوان الالكتروني غير معروف كميا وكذلك نوعيا مثلا عندما يتم إطلاق فيروس لتدمير جهاز حاسب معين لا يمكن التكهن بحجم الخسائر ومداها.

وفي الإرهاب الالكتروني هناك طرق متعددة يستخدمها الإرهابيون في استخدام الكمبيوتر كأداة مثل فيروسات الكمبيوتر أو التجسس أو اختراق المواقع أو سرقة المعلومات وغسيل الأموال وغيرها من الأشكال، وجاء ذلك مع تنوع الأهداف بشكل كبير فيكون هناك هدف فرعي يتفرع من هدف رئيسي، فمثلا يمكن سرقة الهويات الشخصية لإخفاء أعمالهم، وأشاعه الأخبار الاقتصادية التي تؤثر على أداء البورصات العالمية، واستخدام أدوات للتأثير على الاقتصاد الكلي حيث أصبحت الشركات الخاصة وليست فقط الحكومية هي الهدف للتأثير على الاستقرار الاقتصادي والشرعية السياسية.

---

(1)Yonah Alexander, and Donald J. Musch (eds.) **Cyber Terrorism and Information Warfare.** Dobbs Ferry, NY: Oceana Publications, 4 vols, 1999. pp 70-125.

وبدلاً من التدريبات الشاقة وفي ظروف بيئة خاصة كانت تمثل أساس العمل الإرهابي التقليدي، أصبح الإرهاب الالكتروني يعتمد على المهارة في التعامل مع الحاسب والذكاء الفردي، وفي أقل الإمكانيات التي تتمثل في حاسب ووصلة للانترنت فقط والماوس ولوحة المفاتيح، ولم يعد هناك حاجة للسفر آلاف الأميال للتنفيذ مع وجود درجه عالية من الأمان وسهولة الوصول للهدف الذي يتمثل في الشبكات التي تعتمد عليها البنية التحتية الكونية في معظم دول العالم. و كانت الخسائر في الإرهاب القديم محدودة داخل إقليم أو دولة معينة إما لعدم وجود ترابط وتشابك في المصالح بين دول العالم أو ضعف إمكانية تلك الجماعات في إحداث هذه الخسائر الكبيرة مع اعتماد الاتصالات والمرافق الحساسة في دول العالم المتقدم علية وكذلك البورصات العالمية والبنوك والتجارة الالكترونية.

وبما يجعل هناك احتماليه التعرض لخسائر كارثية ودولية في آن واحد، و يميل الإرهاب التقليدي نحو استخدام القوة الصلبة يميل الإرهاب الإلكتروني إلى القوه اللينة بصوره أكبر حيث المعلومات والأفكار والتأثير في الرأي العام مع رخص تكاليف البث وخروجه عن السيطرة الحكومية حيث تحرك الفكرة القوة داخل الفضاء الإلكتروني، أما في الإرهاب التقليدي فإن القوة هي ما تسعى لتغيير الأفكار، ويتم الاستفادة مما يتيحه الفضاء الالكتروني من سرعة الانتشار وتوافر وسائل يمكن استخدامها كأسلحة رخيصة، و نسب النجاح في تنفيذها تكون مرتفعه، وايضاً كوسيلة إعلام رخيصة ومتعددة الوسائط الإعلامية من نص وصوت وصورة وفيديو تخدم على الرسالة الإعلامية.

ويكون هناك طرق متعددة لإصابة العدو من دون وجود أسلحة مادية كأداة مثل استخدام فيروسات الكمبيوتر أو التجسس أو اختراق المواقع أو سرقة المعلومات وغيرها من الأشكال، وقد يقف وراء استخدامها دوافع أخري أقتصادية وثقافية واجتماعية و يتميز الإرهاب الإلكتروني باتساع نطاق وساحة الهجموم مع اتساع شبكات الاتصال والمعلومات في كافة ارجاء العالم، وبشكل لا تعير تلك الهجمات اعتبارا للحدود الدولية أو المسئولية القانونية للدولة عن أعمالها حيث يمكن أن تقوم مجموعه من المهاجمين في عدد من الدول لمهاجمه هدف معين وهذا ما يعني صعوبة تحديد المسئولية القانونية ويمتد مجال تلك الحرب مع تمدد الفضاء الإلكتروني عالميا.

ويكون مجال ممارسة الإرهاب الإلكتروني متسعاً مع اتساع مستخدمي الإنترنت وأدوات تكنولوجيا الاتصال والمعلومات في العالم، وخلافا لأسلحة القرن العشرين المبتكرة والتي تستغرق نحو ١٥ عاما حتى تدخل الخدمة العسكرية فان أحدث الطرازات من أجهزة الكمبيوتر والبرامج الالكترونية والاسلحة الالكترونية متاحة الآن في كل مكان ويمكن كذلك لأي شخص الدخول عليها في نفس الوقت والحصول على معلومات بشأنها واستخدامها مع انخفاض تكلفتها وسهولة نقلها وتطويرها، و أصبح من السهولة انضمام أي مجند جديد إلى أي جماعه إرهابية حيث لا توجد شروط للعضوية سوى الالتزام بأهدافهم وعدم التقيد بطرق التنفيذ وتوفر تلك العضوية مصادر جديدة من المعلومات محلية وكوادر محلية بعيدا عن القيادة المركزية وهذا ما يعكس طبيعة شبكية ولامركزية معقدة وخلايا قد تكون منفصلة عن بعضها البعض مكانيا الا انها تلقتي في الاهداف والافكار وهذا ما يعمل على وجود صعوبة في الملاحقة الأمنية لهم.

١- الارهاب الالكتروني اداة من ادوات ارهاب الدولة وشن الحروب.

وهو ذلك الإرهاب الذي تقوده الدولة من خلال مجموعه الأعمال والسياسات الحكومية التي تستهدف نشر الرعب بين المواطنين عن طريق فرض القيود على الدخول للفضاء الالكتروني في الداخل وصولا إلى تأمين خضوعهم لرغبات الحكومة، أو قد تستخدمه الدولة في التعامل مع غيرها من الدول في الخارج بهدف تحقيق بعض الأهداف التي لا تستطيع الدولة ولا تتمكن من تحقيقها بالوسائل السلمية والأساليب المشروعة، وتستخدم عمليات انتهاك الحرية والخصوصية حينما تغلب اعتبارت الامن على الحرية لمواجهه المعارضين للنظام السياسي فيظهر عمليات حجب المواقع واعتقال المدونيين وغيرها وذلك لبث الرعب في أوساط مجموعه معينه من المواطنين.[1]

وهناك أيضا مستوى خارجي تمارسه الدولة عن طريق القيام بمجموعه اعمال عدائية عبر الفضاء الالكتروني أو إن تقوم عبر أجهزتها بالقيام بأعمال تخريبية ضد مؤسسات ومرافق الدول الأخرى، وفي هذا الحالة نكون أمام إرهاب الدولة المباشر حيث يأخذ شكل حرب باردة لا ترقى إلى تحريك الآلة العسكرية التقليدية، وعلى الرغم من أن الدولة عادة ما تلجأ لممارسة الإرهاب على وجه غير مباشر وذلك من خلال دعمها وتأييدها أو من خلال تجنيد منظمة إرهابية أو جريمة منظمة تستخدمها [2].

ويوجد تيار يؤيد فكرة وجود إرهاب الدولة، كأحد أشكال الإرهاب، استنادًا على أن هناك دول تقوم بممارسات إرهابية حقيقية ضد الأطراف الأخرى، كأعمال الاغتيالات والتخريب المتعمدة، إضافة إلى ما يثار أحيانا بشأن ممارسات بعض الأجهزة الأمنية داخل الدول ضد المواطنين، وهناك بالفعل خلاف مستمر حول الجوانب القانونية لإرهاب الدولة في الجمعية العامة للأمم المتحدةوهناك تيار أخر يقرر أنه لا يوجد شيء اسمه إرهاب الدولة، وأن الوضع القانوني للعمليات التي تقوم بها الدول يرتبط بفكرة أكثر قوة هي " العدوان" المحدد في المواثيق الدولية، إضافة إلى أنه يمكن تكييف الأعمال العنيفة التي تقوم بها الدول، والتي تعتبر متجاوزة، على أنها انتهاكات للقانون الدولي، استنادا على المواثيق المنظمة لالتزامات سلطات الاحتلال، أو قواعد القانون الدولي الإنساني، أو حتى جرائم الحرب التي لا تسقط بالتقادم.

٢- يتوقف التهديد وتقييمه على حملة لنوايا إرهابية:

يتوقف الفعل الارهابي على درجة التقييم للنوايا وقدرات المهاجمين ودوافعهم السياسية وراء محاولة بث الرعب أو إلحاق أضرار ماديه [3]. ومن ثم فان تلك النوايا تصبح واضحة عند الجماعات الإرهابية ويمكن أن يتم توظيف الجريمة لخدمة تلك النوايا وغيرها من الآليات، والتي ربما تكون تحت حالة الرصد من قبل أجهزة الاستخبارات الدولية، كما أن تلك الجماعات قد لا يلجأ معظمها لاستخدام الإنترنت كوسيلة للهجوم وتستخدمه الدول في العمل الإرهابي أيضاً أو كساحة حرب بين الدول

---

(1) د. نبيل علي " عنف المعلومات...وإرهابها " في "مستقبل الثورة الرقمية:العرب والتحدي القادم " نخبة من الكتاب، وزارة الإعلام الكويتية، سلسلة كتاب العربي (٥٥) ١٥ يناير ٢٠٠٤ص ص ٣٠-٤٢.

(2) عبد الناصر حريز، "الارهاب السياسي دراسة تحليلية"، مكتبة مدبولي، القاهرة، الطبعة الاولى، ١٩٩٦ص ص ٢٧٨-٢٣٠.

(3) Kathryn Kerr," Putting cyberterrorism into context", Op. Cit

ويعضها البعض أو تدخل في نطاق المنافسة بين الشركات العالمية حول الابتكارات التكنولوجية، ويفتح المجال لاستخدام الفضاء الالكتروني كوسيلة قتالية اوحربية او هجومية.

وهناك محددات أمام استخدام الجماعات الإرهابية للفضاء الالكتروني تتمثل في أولا: إن الإرهابيين قد لا يكون لديهم القدرة الفنية العالية التي تمكنهم من استخدام أدوات الفضاء الإلكتروني في الحرب، وثانيا: إن استخدام هجمات الفضاء الإلكتروني قد لا تكون وسيلة متاحة لمعظم الإرهابيين.

٣- عدم توافر درجة عالية من اليقين بشأن نتائج تلك الهجمات.

وذلك بالمقارنة بالهجمات التقليدية التي يكون خلالها الموقع المستهدف محدداً والأضرار يمكن توقعها ومن السهل اختراق الموقع المستهدف، كما أن الانتعاشة السريعة من أثار الهجوم يمكن أن تحدث بسرعة غير متوقعه، وقد يتمكن الفنيون من سرعة إصلاح تلك الأعطال، حيث يمكن الكشف عن مصادر الخلل بصورة أسرع والتمكن من تشخيص العطل ثم إصلاحه بشكل لا يعرضه مرة أخرى للضرر وفق نظم حماية فربما يتطلب الأمر إعادة تثبيت نظام التشغيل أو التطبيقات الأخرى الحاسمة، والملفات الاحتياطية، والشبكات الإضافية، وفي مقابل ذلك فإن الهجوم التقليدي عادة ما ينطوي على أضرار جسديه خطيرة وتحتاج إلى إعادة بناء وتعويض عدد من المعدات وتوفير التسهيلات التي من المحتمل أن تستغرق وقتا اكبر وموارد اكبر بشكل يعطي الفرصة لتلقي ضربة أخرى.(١)

٤- القدرة على التخفي وتجهيل مصدر الهجمات.

وذلك لعدم وجود أدلة مادية واضحة كما في حالة الهجمات التقليدية ، وتتوقف القدرة على حسم المعركة من خلال هجوم الفضاء الإلكتروني على مدى الضرر الذي يصيب البنية التحتية للمعلومات محل الهجوم من قبل الإرهابيين، و غيرهم بما في ذلك الموظفون الساخطون، والمنافسون، أو العاطلون أو الباحثون عن الشهرة، أو ربما مع الدول القومية والتي تستخدم برامج حرب المعلومات وهجمات الفضاء الالكتروني في أوقات الحرب والصراع مع غيرها. وتظهر تلك الهجمات في حالة النزاعات الدولية أو الصراعات منخفضة الشدة، وقد تستخدم من قبل نشطاء الإنترنت 'Hacktivism' كشكل من أشكال الاحتجاج في جميع أنحاء العالم مع زيادة أعداد مستخدمي الإنترنت والاتصالات وانتشارها الواسع عالميا، وعادة ما تكون هذه الاعتداءات رمزية تعبيرا عن الاحتجاج، وبالرغم من أنها قد تكون غير قانونيه أو أنها قد لا تستهدف الضرر ولكنها تنقل صورة الصراع الدولي والعالمي.(٢)،

٥- سهولة التعرض للاخطار.

يلعب الحاسب الآلي دوراً كبيراً في تسيير الحياة المعاصرة نظراً لكفاءته العالية في معالجة البيانات، وأصبح يشكل القاعدة التي يرتكز عليها عمل العديد من المرافق الهامة مثل المستشفيات والمطارات والبنوك وغيرها. من البنية التحتية الكونية للمعلومات، غير أن النتيجة الجانبية لزيادة الاعتماد على

---

(1) **D.E. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, (1999)**
( http://www.nautilus.org/info-policy/workshop/papers/denning.html)

(2) Timothy F. O'Hara, **Cyber Warfare/Cyber Terrorism. Carlisle Barracks,** PA, U.S. Army War College, 2004. p.24 .**Also available online at:** ( http://handle.dtic.mil/100.2/ADA424310)

تكنولوجيا المعلومات هي ظهور خطر الانزلاق إلى الفوضى في حالة حدوث خلل في الحواسب الآلية. وهو الأمر الذي يجعل من شبكات الحاسب الآلي هدفاً جذاباً لجماعات الإرهاب الدولية، فإلحاق الخسائر بمدينة من المدن لا يحتاج إلى عمليات معقدة كإطلاق صواريخ أو تفجير سيارات مفخخة، ولكن يكفي تعطيل شبكة الحاسب الآلي الخاصة بمطار المدينة أو ببورصتها حتى تدب الفوضى ."[1]

٦- الأثر التدميري الضخم والأثر النفسي .

حظى الارهاب الالكتروني باهتمام كافة وسائل الإعلام والمجتمع الدولي وصناعه تكنولوجيا المعلومات، كما يتم تناوله كقضية مثيرة من قبل الخبراء والصحفيين والسياسيين، وعلى الرغم من وجود ما يزيد على ١٠٠ تعريف للإرهاب إلا انه يمكن القول أن "إن الخوف من الإرهاب "هو أساس العمل الإرهابي، فالخوف هو عنصر أساسي في الإرهاب عن طريق بث الخوف عن طريق الأفراد والجماعات الإرهابية والتي تسعى إلى التأثير على سلوك الآخرين مع صعوبة التمييز بين الاستخدام الإرهابي لتكنولوجيا المعلومات وبين الإرهاب الذي يستخدم تكنولوجيا المعلومات كسلاح أو هدف للهجوم عبر الفضاء الإلكتروني وشبكات الكمبيوتر والإنترنت، وتبقى مسألة الخوف من حدوث الإرهاب هو "الإرهاب " ولا يعني بالضرورة حدوث العمل الإرهابي بالفعل.

٧- الهجوم المتعمد ذو دوافع سياسية .

يكون هناك عنف ضد أهداف مدنية يقوم به جماعات دون القومية أو عملاء سريين ويختلف الإرهاب الإلكتروني عن الأشكال الأخرى من إساءة استخدام الكمبيوتر كجرائم الكمبيوتر و التجسس الاقتصادي وحرب المعلومات وحتى يختلف عن نشطاء الإنترنت، وقد يحمل الإرهاب الإلكتروني آثاراً مادية ونفسية يمكن أن تكون مجتمعة أو في حالة منفردة فالإرهاب الإلكتروني لا يعني فقط التسبب في إحداث أضرار مادية عن طريق تكنولوجيا المعلومات والاتصال، بل انه قد يتسبب في أضرار معنوية تدخل ضمن الحرب النفسية حيث يتم الهجوم على المعتقدات أو الأفكار أو النسيج الاجتماعي والثقافي بهدف خلخلته وتكسير شبكة العلاقات القائمة، إلى جانب الفعل ذي الأثر المادي المتمثل في استخدام أو محاولة استخدام أي نشاط على الإنترنت أو غيرة من الوسائل التكنولوجية لمسح أو الدخول غير المشروع على واحد أو أكثر من أجهزة الحاسب الآلي باستهداف البنية التحتية القومية للمعلومات وخصوصا في مجال التكنولوجيا التي تجمع قطاعات الكهرباء والاتصالات والكمبيوتروهي من ركائز الأمن القومي الجديد.

والتي تكون معرضة جيدا لتهديدات الحرب الرقمية، وهي تقوم على أساس المصادر التي يعتمد عليها من يريد القيام بهجوم رقمي متوافرة ومنتشرة بين عامة الناس وتتألف من جهاز كمبيوتر ونقطة اتصال بالإنترنت وبذلك تعددت مصادر التهديد ومكان انطلاق العمل الإرهابي[2] وصعوبة التمييز بين الاستخدام الإرهابي لتكنولوجيا المعلومات وبين الإرهاب الذي يستخدم تكنولوجيا المعلومات كسلاح

---

(1) هل تصبح شبكة الإنترنت هدفاً لتنظيم القاعدة؟ ، اذاعه صوت المانيا ، اخر زيارة (٣٢-٣-٢٠٠٧) (http://www.dw-world.de/dw/article/0,1564,1543259,00.html)

(2) Scott Berinato ,the trust about Cyberterrorism, CIO Magazine ,15 Mar.2002 (http://www.cio.com/archive/031502/truth.html)

أو هدف للهجوم، وتشكل كل تلك الخصائص بدون أدنى شك إغراءات لاستخدام الإرهاب الإلكتروني ليس فقط من قبل الجماعات الإرهابية بل كذلك الدول

٨- الحاسب الآلي هو الأداة في القيام بهجمات الارهاب الالكتروني.

يتم شن هجمات الإرهاب الالكتروني لما تتميز به من رخص تكلفة الاستخدام بالمقارنة بتكاليف العمليات العسكرية، ومن يقوم بها هو شخص ذو كفاءة وخبرة فنية، وتكون عبارة عن ضربة إستباقية ليكون المستهدف في موقف رد الفعل، ويكون نشاط الهجوم عابر للحدود متجاوزا الزمان والمكان مما يضفي علية إطارا عالميا، ويعتمد الإرهاب الإلكتروني على الخداع في الارتكاب والتضليل في التعرف على مرتكبيها فلا تترك أثرا خلفها، وهناك صعوبة الاحتفاظ الفني بآثارها إن وجدت ويصعب على المحقق التقليدي التعامل معها.، وأن دوافعه بالأساس سياسية وقد تشترك وظيفيا مع غيرها من جرائم الحاسب ، وتشكل كل تلك الخصائص بدون أدنى شك إغراءات لاستخدام الإرهاب الإلكتروني ليس فقط من قبل الجماعات الإرهابية بل كذلك من جانب أجهزة الاستخبارات في العديد من دول العالم .

٨- التكتيكات والمناورة

يتميز الإرهاب الإلكتروني بكونه عبارة عن هجمات كر وفر بين الخصوم وحيث يبقى الطرف القوى هو من يستطيع أن ينجز الضربة الأولى ويأتي الضعيف متأخرا، وتلك الضربات من شأنها تقوية الدفاعات الأمنية في مواجهتها، وبما يكون له أثر ايجابي في تقوية البعد الأمني والتكنولوجي في نفس الوقت، فقد أسهم قيام الولايات المتحدة في مهاجمه مواقع تنظيم القاعدة إلى أن تمكن التنظيم من تطوير قدراته التي مكنته من إمكانية التخفي والظهور المستتر وإنشاء مواقع بديلة وتطوير وسائل الحماية الخاصة سواء أكان ذلك في شكل تطوير برامج مشفرة وسرية للتواصل بين التنظيم أو في تنمية المهارة الفنية والبشرية القادرة على مواجهه المشكلات الأمنية التي تنتج عن الملاحقات الأمنية لمواقع التنظيم على الشبكة الدولية.

وقد قام تنظيم القاعدة بتطوير برنامج أطلق علية "أسرار المجاهدين ٢ "[1] وهو أول برنامج إسلامي للتراسل الآمن عبر الشبكات، وهو يمثل أعلى مستوى تقني في التراسل المشفر. والبرنامج يمكن تحميله مجانا من موقع منتديات شبكة الإخلاص الذي كثيرا ما ينشر رسائل القاعدة، وأصدر هذا البرنامج الجبهة الإعلامية الإسلامية العالمية في أوائل عام ٢٠٠٧ وهي جماعة مرتبطة بالقاعدة تمارس نشاطها على الإنترنت. ودخول موقع منتديات القاعدة يحتاج كلمة مرور كشكل من تأمين التواصل عبر البريد الالكتروني وغيره من أشكال الاتصالات[2]

---

(1) وذكر الموقع: «قامت مجموعة الاخلاص التقني في شبكة الاخلاص الاسلامية بتطوير البرنامج واصدار هذه النسخة الخاصة دعما للمجاهدين علمة ودولة العراق الاسلامية خاصة يمكن الاطلاع على الموقع (http://alekhlaas.net) (اخر زيارة في ٣٠-٩-٢٠٠٧ )

(2) جريدة الشرق الاوسط ٢٠ يناير ٢٠٠٨.

## المطلب الثالث:

## أدوات ووسائل الإرهاب الإلكتروني وطبيعة الفاعلين

أولا : الآليات والأدوات

بصفة عامة تواجه أنظمة الكمبيوتر أخطار عده تصيب المخرجات في أحد العوامل الثلاثة لها، وهي القدرة على الوصول والسرية و السلامة، فالقدرة على الوصول تتمثل في قدرة الإطراف المخولة على أن تحصل على المعلومات، تلك القدرة قد يجري الحد منها أو أن تزال، إما عن طريق تدمير المعلومات أو البرامج أو الأدوات المادية، أو عن طريق التدخل في نظام الكمبيوتر لدرجة أن يصبح النظام مشكوك فيه وعديم الفائدة، أو عن طريق التدخل في ذاكرة النظام أو في معالجة المعلومات. أو سرقة معلومات دقيقة أو بث إشاعات ويرجع ذلك أيضا إلى شيوع استخدام أجهزة الحاسب وتنوع الأهداف والوسائل والأشخاص، والاهم من ذلك كله انه على المستوى الدولي لم يتم إلى الآن الاتفاق حول مفهوم واضح للإرهاب. و هناك عناصر مشتركة مثل الأفراد أو المجموعات أو المواقع (مادية أو افتراضية ) طرق التنفيذ والأهداف والأدوات والدوافع، وقد انعكس ذلك التعدد على طبيعة الحرب ومفهومها بل امتد ذلك التعدد إلى المستوى الاصطلاحي للكلمة، وهنا يبرز تداخل ما بين الحرب المعلوماتية والإرهاب الإلكتروني فالفرق بينهما قد ينحصر في الشرعية فقط إي الاستخدام المشروع للقوة، حيث تلاشت الخطوط الفاصلة فكلاهما يمكن أن تقوم بهما دولة أو فرد أو جماعة، بشكل يجعل الإرهاب الإلكتروني هو أداة من أدوات الحرب المعلوماتية غير التقليدية، وتعتبر الحرب المعلوماتية من أنواع الحروب غير التقليدية بينما تعتبر الأسلحة النووية والكيماوية والبيولوجية من ضمن أشكال الحرب التقليدية[1]

و يتم استخدام الفضاء الإلكتروني استخداما إرهابيا بصورة غير مباشرة عن طريق تسهيل عملية التنفيذ للعمل الإرهابي عبر توفير المعلومات والحصول على التمويل أو صنع المتفجرات، وهناك أيضا استخدامه لبث الكراهية وترويج الخوف عبر استخدام الفضاء الإلكتروني كوسيلة إعلام دولية لها خصائص مميزة، أو بطريقة ثالثة عن طريق استخدام الأدوات والآليات ذات الطابع الالكتروني في الصراع ويكون ميدان ومسرح تلك الحرب أو العمليات العدائية الفضاء الإلكترونيوقد تأتي تلك النماذج الثلاثة مجتمعه أو من خلال عمل احدها بشكل فردي وصعوبة الفصل بين تلك الأدوات .

الادوات والاسلحة الالكترونية توجد في عده نماذج أهمها:

أولا: اختراق المواقع الإلكترونية، حيث يقوم شخص أو أكثر باختراق موقع مضاد لتغيير محتوياته، أو سرقة معلومات سرية، أو تعطيل الموقع عن العمل، أو الاستيلاء عليه بشكل كامل عن طريق السيطرة على اسم النطاق. وعادة ما يضع المهاجمون – بعد نجاح مهمتهم – رسائل في الموقع تعلن اختراقه، وهي بمثابة الراية التي يرفعها المنتصرون على أرض المعركة، وثانيا:الفيروسات، حيث تنتشر فيروسات الحاسب بسرعة كبيرة من خلال شبكة الإنترنت نظرا للحجم الكبير لتبادل الملفات والبرامج بين

---

(1) Sarah Gordon & Richard Ford ,"Cyber terrorism" .Symantec cooperation .op.cit

مستخدمي الشبكة. وفيروسات الحاسب عبارة عن برامج تستنسخ نفسها في الجهاز المصاب عندما تنشط لتحدث تغييرات في البرامج أو البيئة التي تعمل فيها تلك البرامج مما يؤدي إلى أضرار مختلفة. وتتراوح هذه الأضرار بين رسائل مزعجة تظهر للمستخدم، أو فقد للملفات المخزنة، وقد تصل إلى تحطم نظام التشغيل في الجهاز. وثالثا :الحرب الإعلامية، حيث أصبحت الفضاء الالكتروني وسيلة مهمة للتأثير على الرأي العام ومخاطبة ملايين المستخدمين من خلال النص والصوت والصورة. فيمكن للأفراد و المنظمات تأسيس مواقع على الإنترنت لتكون منابر إعلامية تساعد على إيصال صوتهم للعالم ووضع كل ما يساند قضيتهم أمام المهتمين. ومن ذلك ما فعله الشيشانيون عندما أسسوا مواقع بلغات عدة لشرح قضيتهم وفضح الممارسات الروسية في القوقاز ضد الشعب الشيشاني، وعززوا ذلك بنشر صور وأفلام للمذابح والانتهاكات التي لا تبثها وسائل الإعلام التقليدية (الصحافة والتلفزيون)، أو تعتم عليها، أو تخضعها لمقص الرقيب. ورابعا : التجسس الإلكتروني حيث برعت حكومات كثيرة في استخدام تقنيات متطورة للتجسس على شبكة الإنترنت، ولا سيما أن المعلومات التي تنتقل عبر الشبكات يمكن اعتراضها والتجسس عليها وتنقسم أهداف هجمات الارهاب الالكتروني لثلاثة هي اولا :القيام بهجمات رقمية الطابع عبر وسيط الفضاء الالكتروني حيث يتم شن عمليات التدمير والهجوم الكترونيا . وثانيا: ان يكون الفضاء الالكتروني عامل مساعد في العمل الارهاب عن طريق تسهيل الحصول على المعلومات والتنسيق والتجنيد والتعبئة وغيرها . وثالثا: يتمثل في العمل على شن الحرب النفسية ونشر المعلومات المضللة والكراهية الدينية وما يقابل ذلك من انتهاكات لحقوق الانسان كحجب المواقع او تنفيذ الاعتقالات للخصوم السياسين .

وتشمل عملية تفعيل الإرهاب الإلكتروني عبر أربع مراحل حيث تشمل:

المرحلة الأولى: طرق ووسائل الهجوم والتي منها تعطيل الخدمة - هجوم بالفيروسات - المساعدة غير المباشرة في العمل الإرهابي - المساعدة المباشرة في حرب المعلومات - وأخرى . والمرحلة الثانية :إصابة الهدف وتشمل البنية التحية للمعلومات - المصارف المالية- الحكومات الالكترونية والمرحلة الثالثة: التأثيروالذي يكون لة ابعاد داخليه و خارجية. والمرحلة الرابعة: التداعيات وتشمل انهيار شبكات المعلومات - إصابة المرافق الحيوية - الارتباك العام - خسائر مادية واقتصادية وغيرها .

وهناك العديد من الأدوات والآليات ذات الطابع الالكتروني والتي يمكن إن يتم استخدامها في شن هجمات الإرهاب الإلكتروني والتي تعد في نفس الوقت اسلحة للجهوم ومنها: - القنابل المنطقية والقراصنة والديدان و القرصنة Hackers: أفراد من أوساط الناس أصحاب مهارات كومبيوتريّة عالية، لديهم الرغبة لاختبار قدراتهم، ولذلك يلجئون غالبا إلى إثباتها بطرق غير شرعية.- فيروسات الكومبيوتر Virus: برامج صغيرة تُستخدم لتعطيل شبكات الخدمات والبني التحتيّة لهدف ما، ويمكنها مثلا شلّ، أو على الأقل إحداث فشل عامّ، في شبكة الاتصالات لدولة ما، طالما كانت شبكة اتصالاتها تعتمد على الكومبيوتر. - الديدان Worms: الدودة هي برنامج مستقل، يتكاثر بنسخ نفسه عن طريق الشبكات، وإذا لم تدمر الدودة البيانات، مثل الديدان التي تنتشر عبر الإنترنت، فهي قد تقطع الاتصالات، كما أنها قادرة على تغيير شكلها، وهي غالبا تستهدف الشبكات المالية

التي تعتمد على الكومبيوتر، مثل شبكات المصارف أو البورصات. - أحصنة طروادة Trojan Horses: حصان طروادة هو عبارة عن جزء من شفرة أو برنامج صغير مختبئ في برنامج أكبر، غالبا ما يكون من النوع واسع الانتشار والشهرة. وتؤدي الأحصنة هذه مهمّات خفيّة غالبا ما تكون إطلاق فيروس أو دودة، ولها دور مهم هو إضعاف بيئة الهدف قبل اندلاع الحرب، حيث تقوم بإرسال بيانات عن الثغرات الموجودة في نظام ما، وكذلك إرسال كلمات المرور السرية الخاصة بكلّ ما هو حسّاس من مخزون معلومات الهدف. - القنابل المنطقية Logic Bombs: نوع من أحصنة طروادة، يزرعها المبرمج داخل النظام الذي يطوّره، أو تكون برنامجا مستقلا. وتستخدم الدول في شنّ حرب إلكترونيّة والتلصص والتجسس والوقوف على حالة الدولة المعادية. الأبواب الخلفية Backdoors: هي ثغرة تترك عن عمد من مصمم النظام للتسلل إليه عند الحاجة. وتجدر الإشارة إلى أن الكثير من البرامج والنظم التي تنتجها الولايات المتحدة الأميركية تحتوي على أبواب خلفية تستخدمها عند الحاجة، وهو ما يسمح لهيئات وأركان حرب المعلومات من التجوال الحرّ داخل أي نظامٍ لأي دولة أجنبية. - الاختناق المروري الإلكترونيّ Electronic Jamming: يسمح بسدّ وخنق قنوات الاتصالات لدى الهدف بحيث لا يمكنه تبادل المعلومات. وتمّ تطوير هذه الخطة بخطوة أكثر فائدة هي استبدال المعلومات وهي في الطريق بين الطرف المستقبل والمرسل بمعلومات مضللة.

ثانيا: الفاعلون في استخدام هجمات الارهاب الإلكتروني

أصبحت العلاقة بين القوة والإرهاب متداخلة، فالإرهاب هو عبارة عن استخدام القوة فان الإرهاب في حد ذاته يعد عنصر قوة، ويعد كون استخدام القوة إرهابا يتوقف على مشروعية ذلك الاستخدام من وجهه نظر القانون الدولي، وهذا بالمقارنة بوجهه نظر الدول والتي تختلف حول طبيعة استخدام القوة في حد ذاتها فما يصعب استهدافه مباشرة والعمل على تدميره من الخارج، يتم بدلا من ذلك استخدام القوة المستترة تارة وغير المستترة تارة أخرى بهدف النيل من الأمن الذاتي والفكري وبث الرعب، وذلك حين يعتبر الإرهاب بديلا عن الحروب التقليدية وذلك لفاعلية نتائجه والخصائص التي يتميز بها بالمقارنة بالحروب العسكرية، بل إن الدول تستخدمه وتؤيده ماديا ومعنويا، ويمكن تصنيف المهاجمين باستخدام الإرهاب الإلكتروني إلى أربعه أصناف هم:الإرهابيون و الدول القومية، و المتعاطفين مع مواقف الارهابين أو الدول والجريمة المنظمة والباحثين عن الشهرة. بالإضافة إلى الدول حين تستخدم الإرهاب الإلكتروني كحرب فيما بين الدول وكتعبير عن الصراعات بأنواعها على المستوى الدولي.

١- الإرهابيون:

يتم استخدام الفضاء الالكتروني في التجنيد والتعبئة والتخطيط والتنسيق والتمويل وجمع المعلومات حول تنفيذ العمل الإرهابي أو في استخدام هجمات الفضاء الإلكتروني كسلاح وهدف ضد أعدائها، وتمثل حالة تنظيم القاعدة نموذجا لاستخدام الجماعات "الإرهابية" ودون القومية للفضاء الالكتروني، وحتى اليوم تستخدم مجموعات إرهابية قليلة هجمات الفضاء الإلكتروني كسلاح، وأصبح لدي الارهابين معرفة كافية توضح اهتمامهم بالإنترنت وشبكة الكمبيوتر كسلاح أو كهدف للهجوم ،

وعلى الرغم من انه ليس واضحا حدود استخدامه إلا أن تنظيم القاعدة تمكن من استخدام الانترنت في الحشد والتجنيد والتعبئة والتمويل.

٢- الدول القومية:

لم يقتصر استخدام الإرهاب الإلكتروني على الجماعات الإرهابية فقط بل قد تستخدمه الدولة كاداه للحرب ضد دول أخرى معادية أو أن تستخدمه في مجال الاستخبارات المعادية ضد الدول الأخرى أو قد تقوم الدول بالتعاون مع جماعات إرهابية أو افرد للإضرار بدولة أخرى، وقد يتحول الخلاف السياسي بين دولتين إلى مواجهه عبر الفضاء الإلكتروني، وقد يتطور إلى إحداث أضرار مادية ضخمة خاصة مع تمتع الدول بإمكانيات مادية وبشرية ضخمة بالمقارنة بما يمكن أن تمتلكه الجماعات الإرهابية، وهذا ما يمثل مكمن الخطورة الأكبر في درجة التأثير إلا إن مثل هذا النوع من الصراع قد يتم احتواؤه عبر اتفاق رسمي بين دولتين أما في حالة الجماعات الإرهابية والتي لا تمثل دولاً فيصعب إلزام تلك الجماعات بما تقرره الدول بشكلها الرسمي وقد حدث هجوم الكتروني روسي على استونيا تسبب في شل حركة البنية التحتية، كما تم الإعلان عن حدوث اختراق للبنتاجون ولأربع وزارات ألمانية ووزارة الدفاع الفرنسية ووجهت أصابع الاتهام إلى الصين.

٣- المتعاطفون مع الارهابين ومواقف الدول:

إن إتاحة شبكة المعلومات الدولية للعديد من الأفراد والدول والجماعات على الاتصال والتواصل والتأثر يدفع إلى إمكانية مساهمة أي منها لمسانده دولة أو جماعه أو حتى احتجاج على قضية ما، مع توافر درجة التشابك العالية والاعتماد المتبادل بين دول العالم بالإضافة إلى انه لا تخلو دولة من وجود مهاجرين ينتمون إلى دول أخرى أو بناء شبكة موالين ومتعاطفين مع قضية ما، وخاصة دور الإنترنت في بروز قضايا يتفاعل معها الأفراد عالميا وبعيدا عن وجهات النظر الرسمية كقضية العلاقة بين الإسلام والغرب أو مناهضه العولمة والرأسمالية. فمثلا يروج للحرب الأمريكية على الإرهاب على أنها حرب صليبية ضد الإسلام بما يدفع إلى التحريض على مشاركة المسلمين وفق للانتماء الديني فقط إلى المشاركة في عمل عدائي ضد الولايات المتحدة، أو حتى المختلفين ايدولوجيا مع الولايات المتحدة كمناهضي العولمة والرأسمالية.

٤- الجريمة المنظمة:

الجريمة المنظمة، حيث قد تستغل آليات الإرهاب الإلكتروني في تحقيق أهداف مادية أو مالية أو بالتعاون مع المنظمات الإرهابية في تحقيق أهدافها مقابل حصولها على المال كالمنظمات العاملة في غسيل الأموال أو تجارة المخدرات أو تجارة السلاح.

٥- الباحثون عن الشهرة:

قد يقوم احد الأشخاص أو المجموعات باستخدام آليات الإرهاب الإلكتروني بهدف الشهرة من قبل أشخاص ذوي درجة عالية من الذكاء، وعلى الرغم من أن الأنواع الأربعة السابقة قد ترتبط بالإرهاب بشكل مباشر اوغير مباشر إلا أن هذا النوع الأخير لا يدخل ضمن العمل الإرهابي ولا يرتبط به .

## المبحث الثالث:
## المفاهيم المرتبطة والمتداخلة مع الإرهاب الالكتروني

كثير من الجدل والتباين قد ظهرا حول طبيعه المفاهيم المرتبطة بالارهاب الالكتروني ولعل نعت تلك الادوات بالارهاب لا يحمل قدرا تقييما اكثر من كونه يعبر عن آلية الفعل ومن ثم فاننا نتحدث عن ارهاب الكتروني مشروع واخر غير مشروع ، وظهرت اساليب واختلافات في تناول ذلك الفعل الذي ينطوي على الاستخدام السيئ للتكنولوجيا وظهر ذلك في احد اهم تلك المفاهيم التي تم تناولها الباحث من خلال التعرض في المطلب الاول للإرهاب الالكتروني والجريمة الالكترونية ، واما المطلب الثاني: الإرهاب الالكتروني وحرب المعلومات ويتناول المطلب الثالث: الجهاد الالكتروني والمقاومة الالكترونية والاحتجاج الالكتروني

### المطلب الأول:
### الإرهاب الالكتروني والجريمة الالكترونية

في الواقع إن هناك تداخلا واضحا يكون من شأنه على بعض الناس عدم التمييز بين الاستخدام السيئ للفضاء الالكتروني أو الاستخدام ذو الطابع الإجرامي أو كأداة إرهابية، وهناك عدد من الأنماط قد يمكن اعتبارها جميعا إذا ما وجهت إلى هدف معين وذا أغراض سياسية إرهابا الكترونيا ، أما إذا فقدت تلك الصبغة السياسية فإنها يمكن أن تصنف ضمن كل نمط بصفه منفردة، و تجدر الإشارة إلى أنة يوجد مجالات لسوء استخدام الكمبيوتر والإنترنت والتي قد تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي واستغلالها بطريقة غير مشروعة، أو تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها أو تدميرها كليا أو جزئيا، أو تشمل استخدام الحاسب الآلي لارتكاب جريمة ما، أو تشمل إساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه.[1]

والترابط بين الأعمال الإجرامية والإرهابية وشبكة الإنترنت من المرجح أن يزدهر في المستقبل حيث يتم دمج الجريمة في الإرهاب لتظهر في مؤشرات الأمن بصفة عامه، فان كان كل من الجريمة والإرهاب يتفقوا في الوسيلة إلا أنهم يختلفوا في الغاية التي تحرك كل منهما، ولعل أشهر الجرائم عبر الإنترنت هي إطلاق الفيروسات لما تسببه من خسائر اقتصادية، فقد تسبب فيروس "تميدا" على سبيل المثال في خسائر قدرت ٥٣٠ مليون دولار للاقتصاد الأمريكي وبلغت تكلفه فيروس I Love You مليون دولار وتفيد المؤشرات إلى زيادة الجرائم عبر الإنترنت بنسبة ٤٨٪ عام ٢٠٠٥ [2].

وهناك تعدد في أشكال تلك الجرائم والتي قد تكون مصحوبة وظيفيا بالإرهاب مثل: التجسس الالكتروني، و القرصنة، والجرائم المنظمة، والمواقع التحريضية ضد المعتقدات الدينية، والمواقع المتخصصة في القذف وتشويه سمعة الأشخاص، والمواقع والقوائم البريدية الإباحية، وتزوير البيانات،

---

[1] John Arquilla, David Ronfeldt, (Edited)," **Networks and Netwars: The Future of Terror, Crime, and Militancy**, RAND, 2001.

[2] يمكن الاطلاع على الموقع على الانترنت ، (اخر زيارة ١٢-٣-٢٠٠٨)
(http://www.computerworld.com/securitytopics/security/virus/)

وغسيل الأموال، والقمار عبر الإنترنت، وتهديدات التجارة الإلكترونية، والجرائم الاقتصادية، وانتهاك الخصوصية، وانتحال شخصية الفرد، وانتحال شخصية المواقع، والإغراق بالرسائل، و الحواسب الآلية، والاقتحام أو التسلل.(1)

وتتميز الجريمة الالكترونية بقدرة مرتكبيها الفائقة على إلحاق خسائر كبيرة و تمكنت السلطات اليونانية من القبض على مشبهه به ومطلوب منذ عام ٢٠٠٢ قام ببيع معلومات سرية حول أنظمة التسلح وذلك عن طريق اختراق أنظمة الكمبيوتر، وقدرت خسائر بيعه لتلك المعلومات ٣٦١ مليون دولار حيث قام بيعها لـ ٢٥٠ مشتري عن طريق الإنترنت في كل من ألمانيا وايطاليا وفرنسا وجنوب إفريقيا والبرازيل ودول في أسيا والبلقان، وهو يعد أفضل قرصان على مستوى العالم .(2)

وتأتي الجريمة الالكترونية في عده اشكال منها الإرهاب الإلكتروني والتجسس الالكتروني، و القرصنة، والجرائم المنظمة، والمواقع التحريضية ضد المعتقدات الدينية، والمواقع المتخصصة في القذف وتشويه سمعة الأشخاص، والمواقع والقوائم البريدية الإباحية، وتزوير البيانات، وغسيل الأموال، والقمار عبر الإنترنت، وتهديدات التجارة الإلكترونية، والجرائم الاقتصادية، وانتهاك الخصوصية، وانتحال شخصية الفرد، وانتحال شخصية المواقع، والإغراق بالرسائل، و الفيروسات الحاسب الآلية، والاقتحام أو التسلل وغيرها . وتواجه جهات التحقيق صعوبات في ضبط الجرائم الالكترونية وذلك بسبب أن الجريمة تتم بصورة مستترة لا يلحظها المجني علية، وكذلك غياب الدليل المرئي وافتقاد أثار الجريمة التقليدية وإعاقة الوصول إلى الدليل بوسائل الحماية الفنية، وهناك سهولة في محو الدليل أو تدميره في زمن قياسي (3)

وهناك ضخامة بالغة لكم البيانات المتعين فحصها، كما قد يكون هناك إحجام عن الإبلاغ خشية التأثير الاقتصادي في مجتمع الأعمال بالإضافة إلى نقص الخبر لدى الأجهزة الأمنية وجهات الادعاء والقضاء في هذا النوع من الجرائم. وتقع الجريمة أولا: إذا ما استخدمت شبكة الاتصال كأداة لارتكاب الجريمة مثل الدخول غير المشروع إلى نظام المعلومات للإطلاع عليها أو إرسال فيروسات تجاه شبكة الانترنت، وثانيا قد يتعدى ذلك ويصل إلى حد المساس بحق الحياة في حالة إذا ما تم العبث في المعلومات الخاصة بمكونات حيوية،

وثالثا: إرسال رسائل الكترونية تدعو إلى إيداع أموال أو تحويل مبالغ أو إعطاء أرقام حسابات أو المشاركة في مشروعات في ظاهرها مريح، ورابعا: حالة الترويج لمنتجات غير أخلاقية أو شبكات تجارة الرقيق الأبيض والجنس والمخدرات، وخامسا: حالات التلصص على الآخرين أو التشهير بهم من خلال معلومات ملفقة، سادسا: حالات الدخول على مواقع الأفراد للحصول على معلومات صناعية أو فنية أو أموال أو الكشف عن بيانات تنافسية، وسابعا: استخدام الانترنت في ارتكاب الجرائم المنظمة

---

(1) Todd A Megill,.**The Dark Fruit of Globalization: Hostile Use of the Internet.** Carlisle Barracks, PA, U.S. Army War College, 2005. p.16.

(2)**Greece arrests man suspected of major data hacks**,Reuters, January 25, 2008

(3) Susan W. Brenner, "At Light Speed": Attribution and Response to Cybercrime. Journal of Criminal Law & Criminology ,No 97 ,Winter 2007,pp 379-475.

والإرهابية من خلال تبادل المعلومات المشفرة. وتتعلق مشكلة التعاون الدولي في مجال الجريمة الالكترونية بأنه أولا، لا يوجد إجماع عالمي حول نوعية السلوك الذي يشكل جريمة مرتبطة بالحاسب، وثانيا، عدم وجود اتفاق عالمي حول التعريف القانوني للسلوك الإجرامي، وثالثا، عدم وجود خبرة في الإطار الشرطي ولدى سلطات الاتهام وكذلك المحاكم في مجال الحاسب، ورابعا: عدم كفاية السلطات القانونية في إطار التحقيق والدخول على نظم الحاسب بما في ذلك عدم إمكانية تطبيق سلطات التحفظ على المواد غير المادية مثل البيانات التي تم محاسبتها، خامسا:عدم وجود تناسق في الإجراءات في مختلف القوانين الوطنية التي تتناول التحقيق المتعلق بجرائم الحاسب، سادسا: الطابع العابر للحدود الإقليمية للعديد من جرائم الحاسب، سابعا، عدم وجود اتفاقيات تسلم متهمين واتفاقية تعاون متبادلة بين السلطات وآلية العمل التي تسمح بالتعاون الدولي وكذلك عدم وجود قابلية لإعداد اتفاقيات تأخذ في الحسبان الحركية والمتطلبات الخاصة للتحقيق في جرائم الحاسب. [1]

## المطلب الثاني:

## الارهاب الالكتروني و حرب المعلومات

١: ماذا تعني الحرب المعلوماتية ؟

تعد حرب المعلومات هي" استخدام نظم المعلومات لاستغلال وتخريب وتدمير وتعطيل معلومات الخصم وعملياته المبنية على المعلومات ونظم معلوماته وشبكات الحاسب الآلي الخاصة بها، وكذلك الحماية من خطر الهجوم من قبل الخصم؛ لإحراز السبق، والتقدم على نظمه العسكرية والاقتصادية".، وتنظر وزارة الدفاع الأمريكية إلى حرب المعلومات على أنها الأعمال التي تتخذ لإحراز التفوق المعلوماتي بمساعدة الإستراتيجية القومية العسكرية للتأثير سلبا على معلومات العدو ونظم معلوماته، وحماية ما لديها من معلومات ونظم. [2]

ويعرف "وين وارتو" حرب المعلومات عن طريق فصلها إلى ثلاثة مستويات: شخصية، ومؤسسية، وعالمية. حرب المعلومات الشخصية: يتم فيها الهجوم على خصوصية الأفراد في الفضاء المعلوماتي بالتصنت عليهم ومراقبة شؤونهم الإلكترونية عبر البريد الإلكتروني، ومكتب التحقيقات الفيدرالية الأمريكية له برنامج carnivore الشهير في التلصص على البريد الإلكتروني، والعبث بالسجلات الرقمية وتغيير مدخلاتها المخزونة في قواعد البيانات . حرب المعلومات بين الشركات والمؤسسات: وهي حرب تدور ضمن إطار المنافسة أكثر من العداء والتي قوامها استباحة كل شيء لتعطيل المنافس وتهديد أسواقه، وقد تقوم شركة باختراق النظام المعلوماتي لمنافسها، وتسرق نتائج وتفاصيل أبحاثه، ليس هذا فحسب بل قد تدمر البيانات الخاصة بمنافسها أو تستبدلها ببيانات زائفة في لمح البصر، وتستطيع بعد هذه الجولة من الحرب المعلوماتية أن تجعل الأمر يبدو كما لو كان حادثا أحدثه فيروس كمبيوتري، أما الإعلان عن المكتشف من هذه الحروب فيكون احتمال ضعيف إذ غالبا ما تخشى

---

[1] جريدة العالم اليوم ، صفحة عالم الكمبيوتر ، ١ نوفمبر ٢٠٠٥ .

[2] Dorothy Elizabeth Robling Denning,.**Information Warfare and Security**. New York, ACM Press, 1999. p. 522.

الشركات والمؤسسات التأثير السلبي للإعلام عنها إلى جانب ما لم يكتشف منها وهو أكثر بكثير وغير معلوم مداه . حرب المعلومات العالمية: ينشب هذا النوع من الحرب بين الدول وبعضها البعض، أو قد تشنه القوى الاقتصادية العالمية ضد بلدان بعينها، لسرقة أسرار الخصوم أو الأعداء وتوجيه تلك المعلومات ضده.. وهي حروب قائمة وجارية بالفعل، واللغط المثار حول نظام التجسس الأمريكي- البريطاني أيشلون هو أبرز تجليات تلك الحرب، وكذلك الدول التي تعوزها البني التحتية، لا تستخدم وسائل حرب المعلومات إلا في أضيق حدود؛ إذ يظل دور تكنولوجيا المعلومات هو جعل الأسلحة أذكى والخسائر أقل في الحرب التقليدية؛

وتستغل حرب المعلومات بنية الأمن التحتية الضعيفة الموجودة في كلّ مكان. وتشير إلى الهجمات التي تنفّذ على شبكة الإنترنت مستهدفة بنية الإنترنت التحتية للمستهلك، مثل المواقع التي تؤمن له الوصول إلى الخدمات على الإنترنت. وفي حين تستطيع الدول القومية أن تشارك في حرب الفضاء الإلكتروني والحرب "القائمة على المعلومات"، فإن حرب المعلومات، يمكن شنّها بسهولة من قبل أفراد أو شركات أو جماعات.[1]

وتحمل حرب المعلومات مصطلح Cyber War ومترادفاته:C4I ، I-WAR ، IW، وغالبا ما يُساء فهمها على انها وتعني استخدام الأسلحة عالية التقنية في الجيوش التقليدية، والصحيح أن في حرب المعلومات تختفي المدافع والصواريخ أو تتأخر للخلف، وتتقدم الحواسب للخطوط الأمامية للجبهات، وهي في كل مكان وفي اللا مكان أيضا ولا مجال للالتحام المباشر، وليس من الضروري أن تنشب تلك الحرب بسبب عداء تقليدي، بل قد تنشب مع منافس تجاري أو اقتصادي، أو خصم ثقافي.[2]

وتشير حرب السيبرcyber war إلى تلك المعلومات التي تستخدم وتتكيف مع الاستخدام العسكري في الحرب وأصبحت تلك الحرب مدخلاً مهماً في العمل العسكري خاصة في نوعها ونطاقها، وذلك في حاله الحديث عن الصراعات عالية الكثافة، ففي حرب السيبر يكون فيها قوات عسكرية نظامية ضد بعضها البعض وهي أقرب إلى الحرب الالكترونية، أما حرب الإنترنت فتظهر في بداية الصراع، وفي حالة الصراعات منخفضة الكثافة، وتضم القوات غير النظامية والفاعلين فيها ليسوا بالضرورة دول ، وكلاهما يشير إلى اقترابات شاملة للصراع من حيث الإستراتيجية والأدوات والمبادئ والتنظيم سواء أكان ذلك من أجل الهجوم أوالدفاع .[3] وظهورالحروب بالوساطة أو الوكالة كأن تبيع إحدى المنظمات المتخصصة في الأعمال العسكرية خدماتها المعلوماتية والأمنية إلى بعض الجهات؛ والحروب"السرية" التي تتخذ نكهة خاصة في الفضاء الافتراضي لأنها تعتمد على أنواع متطورة من

---

(1) David J Gruber,.**Computer Networks and Information Warfare: Implications for Military Operations.** Maxwell Air Force Base, AL, Center for Strategy and Technology, Air War College, Air University, 2000. p.29.

(2) هشام سليمان، " حرب المعلومات الوجه الجديد للحروب "، اسلام اون لاين، ٢/٦/٢٠٠١ (اخر زيارة ١٤-٢-٢٠٠٦) (http://www.islamonline.net/Arabic/Science/2001/06/Article2.shtml)

(3) يمكن الاطلاع على الموقع على الرابط التالي (اخر زيارة ٢٤-٥-٢٠٠٧)( http://www.psycom.net/iwar.1.html)

الفيروسات الالكترونية، إضافة إلى هجمات "الهاكرز" المُنسّقة والمعارك التي لا تهدأ بين شركات برامج حماية الكومبيوتر من جهة وصُنّاع الفيروسات المعلوماتية من الجهة الأخرى[1]

ولا تعني حرب المعلومات الاندماج الجيد فقط للقيادة والسيطرة والاتصالات والحاسبات والاستخبارات ولكنها أيضا تعني التأثير الفعال لتلك المكونات فيما بينها والذي يكون من شأنه حفظ احد أنظمة المعلومات من الاستغلال أو الإفساد أو التدمير ويعني ذلك القدرة على القيام بعمل هجومي على مراكز صنع القرار لدى الخصم وعملياته وهيكلة التنظيمي، والعمل على حماية المقدرات الخاصة بعملية اتخاذ القرار، والعمل على إنشاء واستخدام المعلومات لكي تحقق أهدافنا بفعالية.[2]

و تنقسم حرب المعلومات إلى نوعين نمط هجومي ونمط دفاعي، فالهجومي تقوم بت في الغالب الدولة وأجهزة استخباراتها لما تمتلكه من إمكانيات ضخمة تؤهلها للقيام بها، حيث تستخدم حرب المعلومات الهجومية لأهداف سياسية وعسكرية أو لمجرد الإثارة وإطار القدرات، حيث يستحوذ المهاجم على المعلوماتية ونظمها، ويقوم بالتجسس وسرقة البرامج الكمبيوترية، وقد يقوم بتخريب أو تعطيل نظم المعلوماتية. أما الحرب الدفاعية: فهي تعمل على الحد والوقاية من أعمال التخريب التي قد تتعرض لها، وتختلف الوسائل الدفاعية باختلاف أدوات التخريب والمعلوماتية وطبيعة الأضرار التي قد تحدثها.[3]

وتستخدم حرب المعلومات لتحقيق أهداف إستراتيجية عن طريق التأثير أو السيطرة على كل العناصر السياسية والاقتصادية والعسكرية والمعلوماتية، أما على المستوى العملياتي الميداني فإنها تستخدم للتأثير على شبكات الاتصالات والدعم اللوجستي والقيادة والسيطرة وكل الأنشطة والإمكانيات التي يمكن أن تستخدم. أما على المستوى التكتيكي فهي تهدف إلى التأثير على المعلومات وأنظمة البيانات التي تعتمد عليها بشكل مباشر والتي ترتبط بالعمليات العسكرية.[4]

٢- خصائص الحرب المعلوماتية

تكون الأداة في تلك الحرب أو النزاع هو الحاسب الآلي وكذلك الوسيلة وقد يكون الهدف في ذات الوقت، و تقل المخاطر التي يمكن إن يتعرض لها من يقوم بهذا العمل، كما إن العمليات تتم عبر شبكة الإنترنت لما تتميز بت من رخص تكلفة الدخول بالمقارنة بتكاليف العمليات العسكرية، وان من يقوم بت هو شخص ذو كفاءة وخبرة فنية، وتكون عبارة عن بأنها ضربة استباقية ليكون المستهدف في موقف رد الفعل. ، وان نشاطه عابر للحدود متجاوزا الزمان والمكان مما يضفي علية إطارا عالميا، ويعتمد على الخداع في الارتكاب والتضليل في التعرف على مرتكبيها فلا تترك أثرا خلفها . وهناك خمس خصائص لحرب المعلومات، تشير إلى إمكانية تأجيج النزاع واندلاع الحرب،

---

(1) جريدة الحياه اللندنية - ١٠ ايوليو ٢٠٠٧ .

(2) Craig A. Smith. **The World Wide Web of War**. Carlisle Barracks, PA, U.S. Army War College, 2006.pp 18-23.

(3) **Cyber Warfare and Cyber Terrorism**," Edited By: Lech Janczewski, University of Auckland, New Zealand; Andrew Colarik, Consultant, USA,2007 ,pp 120-360.

(4) Michael N. Schmitt, **Wired warfare: Computer network attack and *jus in bello***, RICR Juin IRRC, Vol. 84, No 846 , June 2002 .

وهي إمكانية توسيع دائرة المشاركين بالعمل الهجومي. و إمكانية الوصول إلى أماكن بعيدة الوصول. والإنكار وسهولة الانتشار و التأثير على الأهداف "الجاهزة إلكترونياً".

وتشكل تلك الميزات إغراءات لاستخدامها من قبل العديد من الدول والتي يغلب عليها الطابع الاستخباراتي ، حيث تمتلك القدرات والإمكانيات التي تؤهلها للدخول لهذا النوع من الحرب ، ويمكن القول إن تلك الحرب يمكن أن تتأثر بها بشده الدول المتقدمة والتي يمكن كذلك أن تشن بين بعضها البعض وذلك لضعف البنية المعلوماتية في الدول النامية ومن ثم تضعف إمكانية تعرضها لهذا النوع من الحرب بشكل مباشر وان كانت من الممكن أن تستخدم لضرب أهداف مادية على اقل تقدير

. و تتميز الحرب المعلوماتية والتي يتم بها استخدام الحاسب بان مجالها ليس له حدود. كما إن مداها لا يمكن التحكم فيه كما إن الهدف غير مأمون العواقب كما تتميز بقدرة عالية على الانتشار عبر الحدود لإصابة دولة متعددة، وقد تستغرق تلك العملية دقائق معدودة، وكذلك الأطراف الذي يمكن أن يقومون بها والتي قد تكون دولة معادية أو دولةً صديقة أو جماعه إرهابية أو فردا. وكذلك صعوبة تجاوز الهدف المحدد واردا كون اتساع مجال العمليات التي يمكن أن يكون مسرحا للنزاع المسلح كما إن انتشار تكنولوجيات المعلومات وتداخلها واعتماد اغلب المرافق الحيوية المدنية والعسكرية،

وهذا ما قد يؤدي بالضرورة إلى التعرض للمدنيين الذين تحميهم الاتفاقيات والمواثيق المتعلقة بالحرب، فضلا عن المنشآت المدنية والمنشآت ذات الطبيعة الخطرة. وكذلك صعوبة اكتشاف الهجوم وينفذ الخصم عملية معلوماتية دون أن يعلم الطرف الآخر، فبعض عمليات الخداع الإلكتروني وفيروسات الحاسب الآلي تؤدي إلى إحداث تغييرات طفيفة على طريقة عمل حاسبات أنظمة الأسلحة للتقليل من فاعلية الأسلحة دون أن يشعر المشغلون بشيء غير طبيعي، ولا تكتشف هذه الحالات إلا بعد تفاقم المشكلة و صعوبة تحديد هوية وهدف الخصم ، و تعتبر من الإجراءات الحساسة فردة الفعل في حالة أن الخصم شخص متطفل تختلف عن ردة الفعل إذا كان الخصم دولة ، لذلك غالباً ما تكون ردة الفعل متأخرة وغير حاسمة.

وتتميز الحرب المعلوماتية بتعدد الفاعلين من الدول أو جماعات إرهابية أو أفراد، وكذلك تتعدد الوسائل والغايات وهذا ما كان له أثرا على وجود تداخل بين الحرب المعلومات وغيرها من الأشكال، وفي الواقع هناك تداخلا واضحا يكون من شأنه على بعض الناس عدم التمييز بين الاستخدام السيئ للكمبيوتر أو كأداة إرهابية أو إجرامية واستخدامه كأداة في النزاع المسلح، فهناك عدد من الأنماط قد يمكن اعتبارها جميعا إذا ما وجهت إلى هدف معين وذا أغراض سياسية بانها حربا عسكرية.

ويمكن القول ان هناك علاقة وثيقة بين حرب المعلومات والارهاب الالكتروني حيث ان الفاعلون في الارهاب الالكتروني يمكن ان يستخدموا حرب المعلومات كاداة لتنفيذ اهدافهم وكذلك فان حرب المعلومات قد تتحول في حد ذاتها الى فعل ارهابي اما بمن يقف وراء استخدامها كالجماعات الارهابية او من الخلال الحكم عليها وفقا لطريقة التنفيذ التي تاخذ نفس تكيكات العمل الارهابي ومن ثم فان الباحث يرى ان كل تلك الاشكال التي تعبر عن استخدام غير سلمي للفضاء الالكتروني تعد ارهابا في طرق تنفيذها الذي يعتمد على هجمات الكر والفر والخوف والترويع .

## المطلب الثالث:

## المقاومة الالكترونية والاحتجاج الالكتروني وحرية الراي والتعبير

أولا: الفضاء الإلكتروني واتاحه أدوات جديدة لحرية الرأي والتعبير:

تزامن دخول العالم إلى العصر الرقمي مع تحولات اجتماعية كبرى فعملية إدماج الأفراد في المؤسسات التي تقوم تقليديا بدور بناء الانتماءات والتراتبيات الاجتماعية يبدو وقد أصابها الوهن على أقل تقدير في المجتمعات التي تجاوزت البني التقليدية في التنظيم الاجتماعي، وهو ما اتاح للأفراد بناء انتماءات جديدة والتموضع على جزء كبير من استخدامات هذه التكنولوجيا المتسمة بمرونتها واستخدامها بطرق مختلفة يحكمها اختلاف مسار حياتهم حيث يجد الفرد نفسه أمام تساؤلات عن موقعه وأي الجماعات ينتمي إليها وعن ذاتيته بداخل هذه التراتب الاجتماعي، ويأتي استخدام التكنولوجيا الرقمية عبر صيغ يحكمها التمايز الفردي، ويمكن لمستخدمي الإنترنت المساهمة في إعادة إنتاج المجتمع بصورة جديدة.

وتعمل جميع اختياراتهم على إضفاء صبغه جديدة عالية ليصبح العالم بصدد ثورة اجتماعية مواكبة للثورة التكنولوجية إذا ما مكنت الإفراد من الانفلات الجزئي أو الكامل من المؤسسات التي تتحكم في صناعه منظمة العلاقات والقيم حيث التمكن من القفز على الصيغة التقليدية لعلاقة المنتج والبائع والزبون، وهو ما يسهم في إعادة النظر في القواعد التي تتحكم في هذه الفضاء وظهرت أشكال جديدة من التفاعل بين الأفراد وصيغ الوصول إلى المعلومة وطبيعة علاقاتهم بها، وساهمت الإنترنت من المساهمة في إسقاط احتكار بعض الفاعلين للمعلومات ووسعت من دائرة الوصول إليها فالمؤسسات التي تستمد قوتها ضمن الفضاء الاجتماعي والثقافي من القيام بالدور المحوري في نشر المعلومات. ومن ثم فقد واجهت تحديا أفقدها الكثير من الأهمية الأمر الذي يمس كل فاعلي الصناعة الثقافية التقليدية ابتداء من المطابع ودور النشر مرورا بالمكتبات والصحف وصولاً إلى الإعلام المسموع والمرئي، وجاء ذلك مع بروز الأشكال الجديدة في نشر المعلومات التي تضعف قوتهم واحتكارهم لآليات تقييم وتصنيف المعلومات ويمتد ذلك الأثر إلى فئات اجتماعية تستمد شرعيتها ضمن التراتبية الاجتماعية و مدى كفاءتها في استثمار المعلومات، ومن ثم يوحد علاقات تفاعل قوي بين التكنولوجيا الرقمية من ناحية والبني الاجتماعية والأفراد من جهة أخرى [1].

و لعل من ثمار التكنولوجيا هو المساهمة في بناء ديمقراطية رقمية جديدة حيث السهولة في الوصول إلى صانعي القرار وسهولة المشاركة والتفاعل وكذلك سهولة الحصول على المعلومات والشفافية والرقابة، وأثرت ثورة المعلومات على ممارسة ومفهوم الديمقراطية الليبرالية حول العالم، مما اتاح فرص اكبر للتعبير السياسي الحر والمشاركة السياسية أمام المواطنين، وعملت على تقوية المؤسسات الاجتماعية المعنية بالسياسات الانتخابية مثل الأحزاب السياسية والثقافة المدنية المشتركة و الرأس المال الاجتماعي المحلي والمجال العام المفتوح أمام الأفكار والمعلومات السياسية، من خلال المشاركة في

---

(1) د الصادق رابح " قراءة في الرهانات الثقافية والاجتماعية للتكنولوجيات الرقمية الحديثة " ، مجلة الاذاعات العربية ، العدد ، ٢٠٠٦، ص ص ٨٥ – ٩٤.

المنتديات الحوارية وبرامج الدردشة والإطلاع السريع على الأخبار والتعليقات السياسية والمشاركات بالرأي والتصويت . وأصبح للفضاء الالكتروني دور في المساعدة في تزايد دور المشاركين في قضايا بناء الرأي العام بعيدا عن الهرميات التقليدية. واتسعت مجالات التعبير عن الرأي عبر الإنترنت، واتسعت القدرة على تكوين مجموعات للتواصل بين الأفراد. والحكام والمحكومين وصانعي القرار في السياسة الخارجية و يسعى نشطاء الإنترنت إلى التعبئة السياسية لإضفاء مزيد من القوة السياسية عليهم في مواجهه النظام السياسي القائم والعمل على دولنه قضاياهم وكسب تعاطف المجتمع الدولي وهذا ما قد يعمل على إضعاف شرعية النظام السياسي القائم على المستويين المحلي والدولي.

وتحولت طبيعة الاتصال الكترونيا من مجرد اتصال يتم بين النخبة فقط إلى اتصال يتم بالتفاعل بين النخبة والجماهير، وكذلك إلى اتصال بين الجماهير المختلفة في دول عديدة بعيدا عن رقابة السلطة الحاكمة في بلدانهم، وذلك في مواجهه احتكاره لوسائل الإعلام التقليدية وممارسه وضعف القيود الحكومية على الإنترنت، مما يدفع المعارضين إلى التلاؤم مع تلك القيود في عملية بث الرسالة الخاصة بهم أو في عملية الحماية ضد الرقابة والتخفي تكنولوجيا. فالحوار بين الأطراف يكون حوارا متكافئا وبه طابع الندية بعيدا عن التفاوت في القدرات الأخرى، وتكون درجة اختلافهم واتفاقهم حول الرؤى والقضايا المطروحة، وكل هذا قد يدخل ضمن الممكن والمباح والاستخدام الجيد للتكنولوجيا .

وكانت الحركات الدينية والسياسية لها التفوق في الاهتمام بالإنترنت بسبب طبيعتها السياسية الساعية إلي نشر أفكارها علي نطاق أوسع، واكتساب أكبر عدد ممكن من المؤيدين لها وهو الأمر الذي توفر لها الإنترنت إمكانيات واسعة لتحقيقه في الترويج لرؤاها ، وعدم اقتصار ذلك علي إقامة مواقع ومنتديات ذات طبيعة دعائية مباشرة بل التوسع إلي حد بعيد في إنشاء أنواع مختلفة منها تغطي معظم إن لم يكن كل الاهتمامات الإنسانية بدءا من الترفيه والتسلية مرورا بالأخبار والتحليلات وانتهاء بالفتاوى والأحكام الدينية[1] وعلى الرغم مما وفرته من ميزات ايجابية أوجدت كذلك ثورة المعلومات مخاطر تتعلق بقدرة الأنظمة السلطوية لاستخدام الدعاية السياسية ومراقبة سلوك مواطنيهم في مقابل مساعده نشطاء ودعاه الديمقراطية في تكسير قبضتهم تدريجيا على السلطة، وكذلك ما يتعلق في مساهمتها بسهولة في تقوية أنماط عدم المساواة وعلاقات القوة الموجودة وتعظيم الفجوة .

ويتميز نشطاء الإنترنت بان لهم أجندة سياسية Activisms بخلاف المخترقين والقراصنة Hacktivism ولهم أربعه أساليب كالدخول بإعداد كبيرة لزيارة موقع فيتسبب في ضغط على الموقع مما يمنع آخرين من الدخول إليه وتعطيل الموقع ، أو حملة تفجير الايميلات حيث يتم تفجير الأهداف بآلاف الرسائل في لحظة واحدة مما يعرف بالهجمات الرصاصية، ففي عام ١٩٩٧ حدثت ضد منظمة الاتصالات الدولية ، والتي تقدم خدمات الإنترنت وكانت تستضيف موقع حركة ايتا الانفصالية مما أدى إلى شل عمل النظام ، وضرب الكمبيوتر والدخول إلى المعلومات المختزنة وتسهيلات الاتصال والمعلومات المالية،و إطلاق الفيروسات والديدان والتي تتكون من اكواد مشفرة تنتشر في أجهزة الكمبيوتر وتنتشر عبر

---

[1] جريدة الاهرام ٢٩ -٤-٢٠٠٥ .

الفضاء الالكتروني ."(1) وقد يكون للمخترقين دوافع سياسية فهم يريدون الاحتجاج أو التعطيل ولكنهم لا يريدون القتل أو التشويه، وهذا قد يكون دافعاً لاستغلال الإرهابيين للهاكر، وربما لا يكون واضحا تماما خاصة إذا تمكنت مجموعات من الإرهابيين في استخدامهم وهم أكثر ذكاء وخبرة أو بسعي الهاكر بتصعيد نشاطهم لمهاجمه الأنظمة التي تشغل العناصر الحساسة في البنية القومية مثل شبكات الكهرباء وخدمات الطوارئ والخدمات الإلكترونية.

وتستغل الجماعات الإرهابية المنتديات الالكترونية لجذب الشباب الجدد إلى كوادرهم أو نقل رسائل مشفرة أو ملفات سريه و لا يوجد فصل حقيقي بين تلك الأنشطة سواء أكانت إجرامية على الإنترنت أو تعبر عن نشاط سياسي محموم من قبل كل القوى السياسية والحزبية فكلها تعتبر أدوات نافعة ولكنها قد تستخدم من قبل الإرهابيين أيضا وظهرت أدوات الرأي والتعبير في إطار عملية الانتقال والتحول من حقوق الإنسان المادية إلى حقوق الإنسان الرقمية والتي أصبحت حق من حقوق الإنسان المعاصر حيث تتحرك الأخيرة عبر الوسيط والفضاء الإلكتروني، وأصبحت تلك الحقوق الجديدة تؤشر لدرجة التحول السياسي والحرية لدى العديد من دول العالم.

ومثلما خضعت الدولة كمفهوم للتحدي في سياساتها الأمنية والسيادية تحت نير التغييرات التكنولوجية والاتصالية التي تجتاح العالم أصبحت تعاني بالمثل من تحدي في سياستها الإعلامية مع تخلخل احتكارها لوسائل الإعلام الجماهيري وكمصدر ومنتج ومروج للمعلومة، وظهر الإعلام الالكتروني حيث أصبح للفرد دوراً فاعلا في صياغته وتشكيلة وانتشاره، وظهرت المدونات كأحد روافد ذلك الإعلام الجديد بقدرة الفرد أن يحرر ويبث أي ماده على الإنترنت وصياغتها إعلاميا مع الحرية في اختيار الموضوع وتحرير النص والحجم وتوقيت النشر وسهولة البث وقلة التكلفة مع إمكانية تجاهل المصدر وأصبح ادوات التعبري والراي عبر الفضاء الالكتروني أكثر من مجرد وسيلة لنقل الخبر أو التعليق علية ليصبح لها دورا في معالجته ومتابعته وإثارة ردود الأفعال مع القدرة الهائلة على الانتشار.

ويحمل ظهور الاعلام الالكتروني عملية التفاعل والتعبير عن كافة الاتجاهات وفي صياغة المضمون المعرفي والثقافي وفي تنظيم الصلات والعلاقات لدعم كافة أشكال التعبير المختلفة عن البيئة الاجتماعية والسياسية داخل المجتمع في ظل حوار يكون ركيزته الندية بين الفرد والنخبة والجماهير، ولم تعد تمارس النخبة دورها المعتاد في صياغة الرأي العام وتشكيله وتعبئته، كون المدونات أصبحت أداه للتأثير على احتكار بعض الفاعلين التقليديين للمعلومات، ومثل ذلك شكلا جديدا من أدوات الضغط على الحكومة في سياستها العامة أو شفافية قراراتها أو في أدائها واستجابتها للمنتج الإعلامي ذي الطابع الفردي والقادر على الانتشار و التأثير في الرأي العام.

وأصبحت أدوات الرأي والتعبير تستخدم كأدوات للمشاركة السياسية ويستخدمها نشطاء الإنترنت كاداه في الاحتجاجات والاعتصام والمظاهرات على السياسات الحكومية، ويرجع ذلك إما للبعد عن

---

(1) Dorothy E. Denning , Activism, Hacktivism, and Cyber terrorism:The Internet as a Tool for Influencing Foreign Policy,Op.Cit at( http://www.totse.com/en/technology/cyberspace_the_new_frontier/cyberspc.html)

الاصطدام المباشر بالسلطة في محيطها الضيق داخل الأسرة أو في محدودية هامش الحرية داخل المجتمع أو ضعف القدرة للوصول إلى منافذ التعبير التقليدية أو لاعتبارات تتعلق بجاذبية المدونات كأداه إعلامية، والتي تظهر فيما يطرحه المدونون في أشكال متعددة منها ذات الطابع الساخر ومنها مدونات ذات طابع متمرد على الواقع أو أخرى عشوائية الهدف أو ذات طابع شخصي أو أنها تخدم مصالح حزبيه وسياسية ودينية.

وكذلك ظهرت الصحافة الالكترونية والتي تتميز عن الصحافة الورقية بما يتوافر لها من وسائط إعلامية متعددة ومستمرة ومتجددة بما يساهم في صياغة الرسالة الإعلامية بشكل جيد وسرعة انتشارها و قدرة المدونات على الكشف السريع للإحداث وتغطيتها المستمرة بالمقارنة بالصحف الورقية، وأصبح هناك درجة تأثير وتأثر بين ما يتاح للناس من درجات الحرية والمشاركة وبين اللجوء إلى أدوات أخرى أكثر حداثة وفاعلية.

وتمثل ادوات الراي والتعبير عبر الفضاء الالكتروني نمطا جديدا من المشاركة السياسية سواء للمنتمين للأحزاب السياسية أو المهتمين بالشأن العام، و كوسيلة من وسائل الحشد والتعبئة والتنسيق بين التفاعلات السياسية، وتعكس درجة ما للتفاعل بين الفرد والمجتمع والدولة مما يؤدي إلى الرشادة في صنع قرارات السياسة العامة ونمط جديد من المشاركة السياسية.

ثانيا : الإرهاب الإلكتروني والاحتجاج الالكتروني

يعد الاحتجاج شكلاً من أشكال الضغط غير العنيف على المؤسسات الحكومية أو الرسمية وذلك لتحقيق مطالب معينة ويأتي هذا الضغط في شكل إضراب عن العمل أو وقفات احتجاجية أو أي مظاهر احتجاج يتم الاتفاق عليها، وجاء التزاوج ما بين الاحتجاج كأداة للتعبير عن الرأي والإنترنت كوسيلة وأداة لاستخدام الفضاء الإلكتروني في التنظيم والحشد والتعبئة والتجنيد والتنسيق وشن حملات دعائية، ويأتي هذا في صورة تقديم المساعدة في الشكل التنظيمي والدعائي للاحتجاج التقليدي أو في وجود احتجاج يأخذ طابعا الكترونيا بحتا أو وجود احتجاج يجمع كلا النمطين. وهناك من يحتج على بعض المواد المنشورة عبر الإنترنت والمعادية وكذلك المطالبة بتغيير أوضاع أو سياسات أو احتجاج على اعتقالات أو أحداث بعينها. وظهر ذلك في تناول بعض القضايا ذات البعد الدولي مثل القيام بحملات الكترونية لمقاطعه المنتجات الدنمركية أو الاحتجاج على ممارسات إسرائيل في الأرض المحتلة إلى الاهتمام بقضايا حياتية تعبر عن معاناة المواطن كارتفاع الأسعار وسياسات حكومية محدده ويعمل الفضاء الإلكتروني كوسيط في إجراء الاتصالات بين مؤيدي الإضراب.

وطرح ذلك إمكانية الاستفادة من خبرات شبابية على صلة بتكنولوجيا الاتصال والمعلومات، كما يتميز بدرجة عالية من المرونة والانفتاح على الأخرين في إطار من الرغبة في تحقيق المنفعة العامة، ويتيح الفرصة للتفاعل والاتصال المستمر بين منظمي الإضراب بما ينعكس على تطوير إستراتيجيتهم، وأيضا يتم توظيف الإنترنت في نشر المعرفة والوعي بالقضية محل الاحتجاج، وتوفير وسيط إعلامي سريع الانتشار ورخيص التكلفة وفي متناول فئة عريضة من الشباب عبر تشكيل مجموعات على موقع الفيس بوك أو المواقع الاجتماعية والمدونات ورسائل المحمول المجانية.

وتتركز أهم صور وأشكال الاحتجاج الالكتروني في جمع التوقيعات الالكترونية للمطالبة بتغيير سياسات أو قرارات أو إزالة صور تعد مسيئة أخلاقيا أو دينيا في الفترة الماضية حاز موقع Petition Online شهرة واسعة بصفته المنصة الرئيسية لإطلاق الاحتجاجات و حملات جمع التوقيعات ضد أي شيء و كل شيء، فقد وفر الموقع للناس وسيلة للتعبير عن الرأي و الاحتجاج في بيئة الكترونية سهلة الوصول جعلت من السهل الحصول على ملايين الأصوات لسهولة التواصل عبر الإنترنت.والدخول إلى غرف الدردشة والمنتديات في الإنترنت للقيام بحوارات وتكوين رأي مناصر أو مناهض لقضية من القضايا؛ وتكوين التحالفات السياسية في الإنترنت. ويتم نشر أفكار الإضرابات أو الاعتصام بين اكبر عدد من مستخدمي الإنترنت عن طريق المجموعات البريدية ورسائل المحمول ومهاجمة المواقع الحكومية الالكترونية أو مواقع الخصوم والقرصنة وسرقة المعلومات ونشر الفيروسات وغيرها وإرسال كم كبير من الرسائل الاحتجاجية لكافه الأطراف المعنية بصورة ضاغطة ومزعجة عن طريق البريد الإلكتروني و إنشاء مواقع انترنت لنشر الأفكار والرؤى الخاصة بالموقف الاحتجاجي للحصول على تأييد الرأي العام وتجنيد الموالين والداعمين لفكرة الاحتجاج من جماعات المصالح المختلفة.

ويعد الاحتجاج الالكتروني مختلفا عن الإرهاب في كونه مجرد أداه سياسية للضغط لتنفيذ مطالب معينة في شكل نوع من العصيان المدني ويكمن خلف اللجوء إلية عدد من الأبعاد أهمها: بعد مؤسسي: يتمثل في ضعف دور الأحزاب السياسية والمجتمع المدني وممثلي السلطة التشريعية كمؤسسات وسيطة بين الحاكم والمحكومين، وعدم التوافق بين التغييرات في الرأي العام وبين عملية وضع السياسات، بالإضافة إلى الضغط الخارجي في شكل ارتفاع الأسعار العالمي الذي مثل ضغطا إضافيا.

و بعد تكنولوجي يتعلق بالارتباط المتزايد بتكنولوجيا الاتصال والمعلومات وتوفير فرص أمام لاعبين جدد. وخاصة مع وسيلة سهلة ورخيصة وسريعة الانتشار واندماج الخدمات مع بعضها حيث يتيح الإنترنت خدمة الاتصال والموبيل خدمة الإنترنت وإمكانية التراسل المجاني بينهما فضلا عن الحرية المتاحة وارتفاع سقفها عن وسائل الإعلام التقليدية، وبعد تنموي: إن المجتمعات التي تكون في طور التحول يكون لديها حالة متصاعدة من الحراك السياسي بين المهتمين بالشأن العام، بالإضافة إلى أن انفتاح المواطن على الخارج تجعل لدية طموحات وتطلعات اكبر قد تمثل ضغطا على صانعي القرار وقد لا تتوافق مع الواقع الاجتماعي والاقتصادي.[1]

وبعد ذو طابع جيلي أو عمري حيث إن المجتمعات تشهد ارتفاع معدلات انتشار تكنولوجيا الاتصال والمعلومات تحتوي فئة عمريه من الشباب على دراية كافية بها وتتفاعل معها مقابل الفئات العمرية الأخرى التي ما زال بعضها ينظر إليها بعين المتشكك والناقم عليها ويحاول أن يطبق سياسات أمنية تقليدية لا تصلح مع تطورات العصر.

---

(1) عادل عبد الصادق، "الاحتجاج الالكتروني والفاعلون الجدد في الحياة السياسية "، ملف الاهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالاهرام، العدد ١٦٢، يونيو ٢٠٠٨.

### ثالثا : المقاومة الالكترونية المدلول والهدف وحقيقة الدور

- المقاومة الالكترونية والجهاد الالكتروني

المقاومة الالكترونية هي حرب بلا نار أو دخان وقصف بلا أنقاض وغزو بلا جيوش وميدان للمعركة فسيح لا يقتصر أو يتقيد بمكان النزاع أو المواجهة الجغرافية بل يمتد مع اتساع الفضاء الالكتروني وتخطيه للحدود ولسيادة الدول بما ينعكس على زيادة عدد المهاجمين وزيادة الأهداف المعرضة للقصف ويختلط ما هو مدني بما هو عسكري ويمكن أن يشارك بها المرآة والطفل والشيخ حين تصبح لوحة المفاتيح والفارة للكمبيوتر والاتصال بالانترنت فقط هي مقتضيات الحرب الجديدة.

وتتنوع الأدوات بتنوع آليات التعبير وأدوات التدمير والاختراق في نفس الوقت عبر الفضاء الالكتروني وبما اعتبره الكثير من المشاركين نوعا من الجهاد لا يتطلب التضحية بالمال أو بالنفس و يتسبب في أحداث خسائر اقتصادية ونفسية وتستقطب مواقع الهاكرز شباب من مختلف الأعمار والأجناس والجنسيات ويتم التجنيد والتدريب من خلال إتاحة برامج تعليم كيفية الاختراق والقرصنة حيث يتم عرض مواقع خاصة بالقرصنة ومواقع يقيمها القراصنة ومنتديات اخرى تجمع القراصنة ويتم تبادل الخبرات والمهارات والقدرات .

وتتعلق آليات واستراتيجية الهجوم بنمطين يتعلق الأول بالاستخدام والتوظيف الإعلامي للانترنت كوسيلة أعلام دولية الطابع عن طريق استخدام كافة أدوات الرأي والتعبير عبر الانترنت للتعبير عن وجهات النظر والتأييد، وجمع التوقيعات الالكترونية واستطلاعات الرأي الالكترونية التي تبرز مواقف المشاركين من طرفي النزاع، وغرف الدردشة والمنتديات في الإنترنت للقيام بحوارات وتكوين رأي مناصر؛ وتكوين التحالفات السياسية ونشر أفكار المظاهرات والاحتجاج وإنشاء مواقع انترنت لنشر الأفكار والرؤى الخاصة بالموقف الاحتجاجي للحصول على تأييد الرأي العام وتجنيد الموالين والداعمين وتم إنشاء موقع Palestinianholocaustmuseum.com وهو متحف افتراضي يوثق بالصور المحرقة النازية ضد اليهود في الحرب العالمية الثانية وموقع هولوكوست غزة Gazaholocaustmuseum وغيرها.[1] أما عن النمط الثاني فيتعلق برد الفعل العنيف عن طريق التحول من لغة الحوار والإقناع إلى التدمير والإقصاء عبر القرصنة والاختراق لشل وتعطيل وتدمير الموقع ووقفه عن العمل وإغراقه بآلاف الرسائل الالكترونية، وقد يحمل بعضها فيروسات تؤدي لعرقلة عمل الموقع واختراقه وسرقة المعلومات ونشر الفيروسات، و إرسال كم كبير من الرسائل الاحتجاجية لكافه الأطراف المعنية بصورة ضاغطة ومزعجة عن طريق البريد الإلكتروني، وإظهار حقيقة الدمار والقتل التي تسعى إسرائيل لطمس معالمة من خلال فرض رقابة إعلامية على مناطق القتال وتفعيل الدعوات لمقاطعه المنتجات الأمريكية والإسرائيلية. ويحرك مجموعات المقاومة الإلكترونية الدوافع نفسها التي تحرك المقاتلين على خطوط المواجهة الأمامية في ميدان القتال التقليدي، وتختلف طبيعة

---

(1) عادل عبد الصادق، العدوان على غزة والمقاومة الالكترونية من لغه الحوار الى التدمير "، ملف الاهرام الاستراتيجى، مركز الدراسات السياسية والاستراتيجية بالاهرام، العدد ١٧٠، فبراير ٢٠٠٩

هـؤلاء المهاجمين وفق انتمائهم الايدولوجي فهم ليسوا مثل القراصنة الآخرين الذين هدفهم السرقة أو جمع المال أو حب الظهور ولكنهم قد يتحالفوا مع القراصنة لتحقيق أهداف مشتركة.

أما الجهاد الالكتروني هو شكل من أشكال الحرب التي تشن عبر شبكة الانترنت، وهذه الحرب تستند إلى أسس أيديولوجية وتسعى لتحقيق أهداف محددة. وهي تنفذ بشكل دقيق ومنظم على شبكة الانترنت، وعن طريق مراجعة الشبكات الالكترونية يتبين أن القراصنة الإسلاميين على الشبكة الالكترونية يحافظون على التواصل فيما بينهم بشكل ثابت يتشاركون المعلومات، ويتبادلون الخبرات، ويتناقشون حول الإستراتيجيات المتبعة والأهداف المفترضة والمشروعة. كما أن هناك أدلة أخرى تدل على تزايد التنسيق فيما بينهم في تنفيذ الهجمات حيث السعى الى ان يصبح المجاهدين، قوة إلكترونية هامة قادرة على إنزال الأضرار الجسيمة وأكثر بكثير من تلك التي قد يسببها هجوم إرهابي تقليدي ، ولا يزال الجهاد الالكتروني كما يبدو في مراحله الأولى وتدرك تلك الجماعات القدرة الهائلة التي يمكن توظيفها عبر الفضاء الالكتروني كأسلوب جديد يسعون باستمرار لتنمية مهارتهم في استخدامها لخدمة أهدافها السياسية، وتتحد تلك الجماعات في استراتيجيها الا انها تختلف في طرق تنفيذها حيث يسعى أفراد تلك الجماعات أو غيرهم من المتعاطفين معهم إلى اخذ السبق في مجال تنفيذ عمليات لتخريب المواقع وقد يأتي هذا في شكل تكوين مجموعات موالية عن طريق المنتديات ومواقع الانترنت أو حتى التحالف مع القراصنة لزيادة المعرفة الكافية بطرق الاختراق والتدمير.

أما الجانب الأخر فقد فطنت الجماعات الإسلامية لأهمية الإعلام كعنصر من عناصر المعركة ضد ما تراه محاولة للدفاع عن ذاتها وقيمها وأفكارها ويعزز في الوقت نفسة من انتشارها وتأثيرها في الرأي العام العالمي ويخلق في الوقت نفسة جبهة إعلامية تستطيع أن تخترق سيطرة الإعلام الغربي وتقدم نظرة مغايرة للواقع ومستند إلى مصداقية النص والصورة باستخدام كافة الوسائط الإعلامية التي تميز بها الفضاء الالكتروني بالاضافة إلى رخص تكلفة استخدام وحجم انتشاره عالميا، حيث أدركت تلك الحركات أهمية الرأي العام كأداة ديموقراطية في الغرب وقدرتة على تغيير ما تراه سياسات معادية لها، وجاء ذلك أيضا كمحاولة للالتفاف على السيطرة الحكومية التقليدية على الإعلام وبما مثل متنفسا للتعبير عن معارضتها سواء للنظام السياسي الحاكم في بلدانها أو ضد سياسات لقوى عالمية.

وكان تنظيم القاعدة من انجح الجماعات في استخدام الفضاء الالكتروني كساحة حرب بديلة بين التنظيم واعدائة ودخلت كافة الجماعات السياسية أو الدينية في هذا المضمار، حيث يستخدم لشن هجمات الكر والفر التقليدية التي تستخدم في حالة عدم وجود تكافؤ في القوى بين الفرقاء وكان لحركة المقاومة الإسلامية حماس اهتمام واضح بأهمية الأعلام في معركتها مع إسرائيل وظهر ذلك في تدريب كوادرها على الحرب الالكترونية والحرب عبر الفضاء الالكتروني ، والتي تحمل مدلولات الحرب ولكنها ليست بحرب تقليدية حيث نار بلا دخان وقصف بلا أنقاض وغزو بلا جيوش وميدان للمعركة فسيح لا يقتصر أو يتقيد بمكان النزاع أو المواجهة الجغرافية بل يمتد مع اتساع الفضاء الالكتروني وتخطيه للحدود ولسيادة الدول بما ينعكس على زيادة عدد المهاجمين وزيادة الأهداف المعرضة للقصف في ذات الوقت .

- <u>التحول من الفعل الفردي إلى الجماعي المنظم :</u>

وذلك عن طريق إنشاء العديد من المواقع التي تعمل كمنبر إعلامي مثل مجموعه ألانصار [1]، ومنظمة فرسان الجهاد الإلكتروني، و مجموعة الجهاد الإلكتروني، ومجمع القرصان الإلكتروني المسلم، هذا بالإضافة إلى العديد من المواقع والمنتديات التي تهدف إلى التجنيد والحشد والتعبئة والتواصل وتبادل الخبارت والتنسيق ،هذا إلى جانب شرح طبيعة الجهاد الالكتروني و إستراتيجيته وشرح الطرق الفنية المستخدمة في شن الهجمات الالكترونية. بالإضافة إلى عرض الإنجازات والدعوة للتعاون ومحاولة استقطاب أعضاء جدد. تدل على مدى تطور الطبيعة التنظيمية للجهاد الإلكتروني ظهرت من خلال مبادرة أطلقت في الثالث من شهر يناير٢٠٠٧ على شبكة المواقع الإسلامية، حيث دعي المجاهدون العاملون على شبكة الانترنت والعاملون في ميدان الإعلام بشكل عام، إلى توقيع معاهدة أطلق عليها اسم حلف المهاجرين(Pact of the Immigrants )، والتي يلتزم بموجبها الجميع على الوقوف موحدين تحت علم وراية ألوية المهاجرين، لتوسيع ونشر المعركة على شبكة الإنترنت. والعمل على مهاجمة المواقع التي تشكل خطراً على الإسلام والمسلمين، وهذه المبادرة تظهر بوضوح أن قراصنة الشبكة الإلكترونية من الإسلاميين لم يعودوا ناشطين متفرقين واصبحوا تحت راية حلف يجمعهم ويربطهم [2].

- <u>الفاعلية والتأثير واستراتيجية الهجوم :</u>

يستهدف المجاهدون ثلاثة انواع من المواقع هي :الاولى : المواقع العقائدية التي تنشر المعتقدات،والمبادئ، والأفكار التي يرى المجاهدون أنها لا تتوافق مع المذهب الإسلامي السني،كالمواقع المسيحية، والشيعية، والصهيونية ،والثانية المواقع التي يرى المجاهدون أنها معادية للإسلام، ومعظم هذه المواقع، هي منتديات خاصة، إخبارية وغير إسلامية.والثالثة الشبكات التي يرى المجاهدون أنها تتناقض مع رؤيتهم الدينية الشاملة، خاصة تلك الشبكات الرياضية الخاصة بالفتيات. أما فيما يتعلق بالشبكات الحكومية وتلك المتعلقة بالأنظمة الدفاعية، والمصالح الاقتصادية الغربية، فإن المواقع الإسلامية لم تظهر أو تعطي أي مؤشرا على أن المجاهدين قد قاموا بالفعل باستهدافها .إلا أن هناك اهتماماً يظهره البعض حول بعض المواقع الحساسة والهامة، و هناك تعاونا بعرض المواقع التي يمكن ان تدخل في استراتيجية الهجوم الالكتروني ووضعها في قائمة يتم تبادلها فيما بينهم .

وتتعلق استراتيجية <u>الهجوم</u> بأن يتم القيام بشل وتعطيل المواقع المستهدفة بزحمة من الاتصالات تؤدي إلى عدم قدرة هذه المواقع على الاستيعاب، بشكل يؤدي إلى إغلاق المواقع بوجه المستخدمين الإضافيين، وفي بعض الأحيان إلى تدمير الموقع ووقفه عن العمل .الثاني: برنامج خاص يقوم على إغراق الموقع بآلاف الرسائل الالكترونية، وقد يحمل بعضها فيروسات تؤدي إلى عرقلة عمل الموقع على الشبكة وتلويثه .البرامج التي يستعملها المجاهدون في هذه الحالات هي إما برامج متوافرة لكافة قراصنة الشبكات الالكترونية بشكل عام، أو برامج وضعت خصيصاً لقراصنة الشبكة الإسلاميين.

---

(1) موقع شبكة الانصار يمكن زيارتها على الانترنت( http://www.al-ansar.virtue.nu/j-e.html) (أخر زيارة ٣-١-٢٠٠٩)

(2) E. Alshech," **Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad**",MERMEI,No.239,Febrauary 2007.

# الفصل الثالث:

# تداعيات الإرهاب الالكتروني على الصراع والأمن الدوليين

## الفصل الثالث:

## تداعيات الإرهاب الالكتروني على الصراع والأمن الدوليين

أصبح للفضاء الالكتروني دورا في التأثير على طبيعة الصراع و القوة التي تمارس من خلاله بالإضافة إلى طبيعة النتائج والآثار التي تنتج عنه ، وهذا ما يعبر عن نوع جديد من ممارسة القوة عبر شكل جديد من أساليب الحرب الالكترونية عبر الفضاء الالكتروني، واثر ذلك على طبيعة القوة المسلحة ويأتي هذا مع خطر انتقال ساحة المواجهة في الحرب من الفضاء الواقعي إلى الفضاء الالكتروني ، وممارسة عمليات الدفاع والهجوم وعلى الجانب الأخر عمل الفضاء الالكتروني على القيام بدور ايجابي على تقليل حدة الصراعات ونشر مبادرات السلام وتعزيز الحوار والتعاون بين دول العالم والانفتاح العالمي على الثقافات المختلفة واستعرض الباحث ذلك عبر ثلاثة مباحث يتعلق الأول بأبعاد وملامح تهديد الإرهاب الالكتروني لأمن المجتمع الدولي ، واما المبحث الثاني فيتناول الإرهاب الالكتروني كشكل جديد من أشكال الصراع الدولي ، واما المبحث الثالث فيتناول طبيعة أنماط استخدام الفضاء الالكتروني في الصراع الدولي .

# المبحث الأول:
# أبعاد وملامح تهديد الإرهاب الالكتروني
# لأمن المجتمع الدولي

**في هذا المبحث يتم تناول ابعاد وملامح تهديد الارهاب الالكتروني لامن المجتمع الدولي ويتم ذلك من خلال التعرض لملامح التاثير والتفاعل المتبادل بين تلك الظاهرة والبنية التحتية الكونية للمعلومات وكيف مثل الفضاء الالكتروني ساحة جديدة للصراع الدولي وظهور نمط جديد من الارهاب عن طريق التزاوج ما بين التكنولوجيا والارهاب ويتم التعرض لذلك من خلال ثلاثة مطالب يتعلق لأول: بالبنية التحتية الكونية للمعلومات وتغير طبيعة الأمن الدولي ، وأما المطلب الثاني فيستعرض الفضاء الالكتروني كساحة للصراع والتنافس الدولي.، ويتناول المطلب الثالث: الإرهاب الجديد والتزاوج ما بين التكنولوجيا والإرهاب.**

## المطلب الأول:
## البنية التحتية الكونية للمعلومات و تغير طبيعة الأمن الدولي

تتعرض البنية التحتية الكونية للمعلومات للخطر عندما يتم قطع خدمة الانترنت أو ضرب مواقعها أو توقف رسائل البث الإذاعي أو التلفزيوني أو توقف موجات الراديو أو سقوط شبكات المحمول أو البث الفضائي وتعطل الخدمات المدنية الهامة، وذلك نظراً لاعتمادها على شبكات تكنولوجيا الاتصال والمعلومات، وأصبح لها تأثير عميق على المجتمع والاقتصاد على النطاق الدولي و الهيكل الاجتماعي والسياسي، أو على دورها في التأثير على أنماط الإرهاب ومستقبلها، وكذلك تأثيرها على طبيعة العلاقات الدولية.

وبعد أحداث ١١ سبتمبر٢٠٠١ أصبح التركيز على الخطر الجديد الذي يمثلة الارهاب الالكتروني يتخذ في بدايته بعدا سياسيا بالتركيز على الظاهرة باعتبارها تدخل ضمن اهتمامات الأمن القومي وأمن الفضاء الالكتروني، وانتقلت القضية بعد ذلك لتتعدى العامل السياسي لتأخذ بعدا اقتصاديا وتمحور الاهتمام حول الأمن الالكتروني، وتأثير ذلك على الاقتصاد الرقمي الجديد الذي يشكل قاطرة النمو الاقتصادي في الدول المتقدمة، وإلى جانب الصناعات التي من الممكن أن تتعرض لتلك المخاطر لينتج عنها خسائر محتمله في الاقتصاد والأرواح.

وزادت حالة الانكشاف الأمني للدول وذلك باعتمادها المتزايد على الفضاء الالكتروني كبرنامج الحكومات الالكترونية والتي تصبح عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات أو إتلافها والتي أصبحت معطاً جديداً للأمن القومي ومن ثم اختلف مفهوم الأمن بتحوله إلى نوع جديد يعتمد على الشبكات والإنترنت ويقع ضمن مهددات الأمن القومي، ودفع ذلك لبروز الخوف من ممارسة الدول لمثل تلك المعطيات إلى جانب الخوف من دور الجماعات الإرهابية في التأثير على الفضاء الالكتروني، وعلى الرغم مما وفره الفضاء الالكتروني من إمكانية لتواصل الفرد مع الآخرين إلا أنها زادت في الوقت نفسه من عزلة الفرد داخل مجتمعه سعيا وراء عالمة الخاص الذي يتلاءم مع ميوله واتجاهاته التي قد لا

تتفق مع ما يحيط به، وهذا ما قد يعمل على الاصطدام بين ما يريده الفرد وما يريده المجتمع ويفرضه من قيود. وعمل الفضاء الالكتروني على الكشف المستمر عن مطالب واحتياجات المواطنين والتي تكون بشكل يفوق قدرة النظم السياسية على تلبيتها مما قد يبدو على أنه عجز وفشل تلك النظم في تلبية مطالب جماهيرها، الأمر الذي قد يدفع للشعور بالإحباط المولد للعنف وقد شهدت اوربا الغربية إبان تحولها ظهور العديد من الجماعات الإرهابية والتي ما لبثت أن تداعت بعد مرحلة الانفتاح السياسي والاقتصادي الذي استطاع أن يمتص تلك الجماعات وساعدت على دعم الاستقرار السياسي بها وتمخض عن الثورة التكنولوجية ثورة أخرى هي الثورة في الشؤون العسكرية وتطور تقنيات الحرب بشكل أصبحت أداة من أدوات حروب المستقبل.(1)

وتعلقت بدور ودقة وحداثة المعلومات في تنافسية الأسلحة والأجهزة العسكرية، وسيطرة دول أخرى على أنظمة الأسلحة والأجهزة العسكرية في عدد من الدول خاصة ما يتعلق بنظام الملاحة العالمي (GPS) وأنظمة الاتصالات والاستطلاع بالأقمار الصناعية، وأصبحت تمتلك الدول التقنية وتستخدم العمليات المعلوماتية كسلاح ردع وتسيطر على أنظمة المعلومات العالمية، وجاء ذلك مع ضعف السيطرة على انتشار المعلومات، حيث يزداد القلق لدى الدول المتقدمة من تعرضها لعمليات تخريب لبنيتها التحتية للمعلومات (2).

وعلى المستوى المدني هناك قابلية البنية الأساسية الحرجة التي تعتمد في عملها على الشبكات وتكنولوجيا الاتصال والمعلومات للتعرض لهذا الخطر، والتي تتراوح ما بين الاتصالات إلى خدمات الطوارئ ومن الصفقات المالية إلى العمليات العسكرية والخدمات الحكومية وخاصة مع اندماج الخدمات حيث التحويلات المالية عبر الهاتف المحمول وخدمة الانترنت وأداء البورصات العالمية وتقديم الخدمات التكنولوجية والتجارة الالكترونية وهذا ما قد يتسبب في حالة انقطاع الكابلات البحرية في احداث خسائر اقتصادية ضخمة.

وأصبح هناك عدة محددات تدفع لتصاعد استخدام العنف وممارسة القوة بسبب انتشار المجال والمدى وتعدد الأطراف داخل مجتمع المعلومات العالمي وتصبح البنية التحتية الكونية للمعلومات التي تعتمد على أنظمة الكمبيوتر معرضة لأخطار عده تصيب القدرة على الحفاظ على الوصول والسرية و السلامة، فالقدرة على الوصول تتمثل في قدرة الإطراف المخولة على أن تحصل على المعلومات، تلك القدرة قد يجري الحد منها أو أن تزال كليا، أما عن طريق تدمير المعلومات أو البرامج أو الأدوات المادية، أو عن طريق التدخل في نظام الكمبيوتر لدرجة أن يصبح النظام مشكوكا فيه وعديم الفائدة، أو عن طريق التدخل في ذاكرة النظام أو المعلومات.

من جانب أخر فإن الحصول على معلومات دقيقة وفورية يمثل ميزة تنافسية، وتصبح عدم إمكانية الحصول على معلومات دقيقة أمراً أسوأ من تدمير هذه المعلومات، وهناك تنوع وتعدد في الفاعلين، وتنوع

(1) Jennie M. Williamson." **Information Operations: Computer Network Attack in the 21st Century**", Carlisle Barracks, PA, U.S. Army War College,2002. pp 15- 22.
(2)T. G. Lewis, " **Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation**" . Hoboken, NJ, Wiley-Interscience,2006. pp 230- 474 .

في الأهداف ويتم توظيف الهجمات بشكل بسيط ورخيص وبشكل متسع في مجال التأثير، كما إن الإشارات التي تحذر من الهجوم تكون متاحة فقط عندما يتم التزود بها، كما إن عملية احتوائه تكون صعبة التحديد، وتبادل هجمات الكر والفر الكترونياً على مواقع العديد من الدول. واتخذت تلك الحروب أشكالاً جمعت بين الضربات الاستباقية التي تهدف لمواجهة تهديد محتمل؛ والحروب بالوساطة كأن تبيع إحدى المنظمات المتخصصة في الأعمال العسكرية خدماتها المعلوماتية والأمنية إلى بعض الجهات؛ والحروب"السرية" التي تتخذ طابعا خاصاً في الفضاء الإلكتروني لأنها تعتمد على أنواع متطورة من الفيروسات الالكترونية، إضافة إلى هجمات "الهاكرز" المُنسّقة والمعارك التي لا تهدأ بين شركات برامج حماية الكومبيوتر وصُنّاع الفيروسات المعلوماتية من الجهة الأخرى[1]

وتستهدف بعض الدول والمنظمات خصومها على الإنترنت استناداً إلى اعتبارات عدة مثل الصراعات الاجتماعية – السياسية كالتي تخوضها عادة الجماعات المناهضة للعولمة ورموزها الاقتصادية مثل"البنك الدولي". وكذلك الحال بالنسبة إلى الصراعات الاثنية والعرقية كتلك المندلعة في بعض المناطق المتوترة مثل كوسوفو والأراضي الفلسطينية المحتلة وبين الهند وباكستان وتايوان والصين وغيرها. وتتميز حروب المواقع بين هذه الفئات بالتدمير المتبادل، وبالاحتلال المؤقت من احد الخصوم لموقع الآخر، وبنشر الدعاية المعادية له. وخاصة مع إتاحة الفرصة للاتصال المتبادل بين الناس في جميع دول العالم بما يعزز من انتشار الأنشطة غير السلمية للفضاء الالكتروني، وتعبر تلك الأنشطة عن استخدام هجمات الفضاء الإلكتروني كنمط للإرهاب والحرب يمكن أن تنتشر بامتداد الفضاء الإلكتروني وتجاوزه الحدود الدولية.[2]

وحدث دمج بين الفضاء الالكتروني مع التكتيك المستخدم في الصراع، وأصبحت حرب المعلومات عبارة عن عمليات حربية تدور في ميدان تكنولوجي رفيع المستوى، حيث يستخدم الطرفان وسائل تكنولوجيا المعلومات للحصول على المبادأة في ميدان المعركة بوحدات كمبيوترية كوحدات أساسية في القوات المسلحة، وذلك بالاستخدام الصحيح والمتقن لجميع الأسلحة المعلوماتية ولتصبح الارهاب الالكتروني يتم عبر صراع الكتروني بين القيادات الصديقة والقيادات المعادية بهدف التاثير على قدرات الخصم واختراق كيانه الالكتروني، واستخدام المعلومات كسلاح رئيسي وحاسم لمهاجمة جهاز المعلومات المعادي وإفشاله في إطار حرب المعلومات.[3]

وقد تقوم دولة بعملية اختراق لنظم المعلومات والبنية التحتية الحيوية لدولة ما بما يمكنها من السيطرة عليها والتحكم في طريقة عملها أو إحداث ضرر أو عمل ما يوقفها عن القيام بعملها، كما يمكن أن تقوم دولة أو غيرها من الأطراف أن تقوم بقصف المواقع الالكترونية الحكومية الخاصة بدولة ما بفيروسات وغيرها من الأسلحة التي يمكن استخدامها في الفضاء الإلكتروني، كما يمكن

(1) Bonnie N. Adkins, ," **The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?"**, A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, Maxwell Air Force Base, Alabama, April 2001
(2) Myriam A. Dunn," **The Internet and the Changing Face of International Relations and Security"**, Volume number; 7, Issue number: 1, ProCon Ltd., Sofia, Bulgaria, 2001
(3) Wang Baocun and Li Fei," Information Warfare" Liberation Army Daily, June 13 and June 20, 1995

لدول ما أن تفرض حصارا على دولة ما عن طريق قطع كابلات الإنترنت أو التشويش على الاتصالات أو منع الدخول أو عملية الحجب لمواقع على الإنترنت. وساعد الفضاء الالكتروني على أن تكون دولة ما مكاناً لانطلاق عمل الاعتداء ضد دولة أخرى خارجية مع عملية الربط بين شبكات الكمبيوتر والإنترنت بين دول العالم، وتجاوزها للحدود التقليدية وسيادة الدول، ولم تعد الدول المعتدية في حاجة إلى إرسال عصابات أو جماعات مسلحة أو الدفع بمجالات التجسس وتجنيد العملاء عبر الفضاء الإلكتروني بهدف اختراق الدول الأخرى، كما إن تلك الحرب يمكن أن تشن من خلال الجيش والمجتمع بما يمثل أسلوباً عسكرياً غير نمطي لإدارة الصراعات المسلحة من خلال اشتراك منظمات غير حكومية وأفراد مدنيين عبر الفضاء الالكتروني ، وجعل ذلك من الصعب تحديد مواقع المتحاربين في ميدان الحرب، حيث إن القطاع المدني المشترك في الحرب واسع وضخم ومن المستحيل تحديد حجمه وأبعاده، ويصبح المبرمجين والهواة والمتعاطفين مع مواقف الدول أو الجماعات الإرهابية بامكانهم إدارة الحرب من اجل تحقيق أهداف وغايات مشتركة تتعلق بتحقيق مصلحة قومية بشكل حافزاً يدفع الجميع لبذل أقصى جهودهم لتحقيق النصر والدفاع من اجل تحقيقها، كما أن الجنود ليسوا فقط مؤهلين للقتال واستخدام أسلحتهم في الميدان، ولكن يجب أيضاً أن يكونوا مؤهلين علمياً وتكنولوجياً لاستخدام أسلحة متطورة تكنولوجياً"(1).

واذا كان الكثير من الدول تستطيع خوض حروب حقيقيّة والانتصار فيها، فان الفوز في الحروب الإلكترونيّة عبر الفضاء الالكتروني صعبة الفوز بسبب عدم معرفة ماذا سيحدث، ومن أين ومتى وكيف وما هو حجم "الجيش" الذي ستواجهه الدول وما هي طبيعة التداعيات التي قد تسفر عن المواجهة وكيف يمكن تحجيمها، وما هو مقدار تكرار الهجمات بما يعكس وجود فوضى أمنية داخل الفضاء الإلكتروني، وبما ينعكس على أمد الصراع خاصة مع سهولة عمليات الاتصال والتخطيط وتسيير العمليات بشكل دقيق وضعف مراقبة سيل المعلومات الهائل الذي يسير بشكلّ يوميّ عبر الفضاء الإلكتروني، كما إنّه بالإمكان إخفاء المعلومات وراء غطاء بريءوجاء استخدام الفضاء الالكتروني كنمط من استخدام القوة عن طريق التأثير على عمل مصادر المعلومات وإتلافها وأنظمة الاتصالات عن طريق الهجوم الالكتروني أو هجوم المعلومات من خلال الأدوات والوسائل الالكترونية بما يؤدي إلى شلل هذه الأنظمة وتدمير أنظمة التشغيل الخاصة بها والتأثير على تدفق المعلومات بما يؤدي إلى إرباك عمل البنية التحتية الحيوية.

وهناك محاولة السيطرة الواسعة على المؤسسات الحيوية للدول الأخرى عن طريق استخدام أسلحة تكنولوجيا الاتصال والمعلومات ضد المنشآت المدنية والعسكرية وأنظمة الدولة والمؤسسات السياسية وإفساد عملها بما يمثل تهديدا مباشرا للأمن القومي الذي يتمثل في الدخول غير المشروع في المؤسسات المالية والاقتصادية والتدمير الواسع للبنية التحتية للاتصالات من خلال استخدام تكنولوجيا الاتصال والمعلومات بما يعد هجوماً على أنظمة صنع القرار والسيطرة والهجوم على الأنظمة الدفاعية للدولة

---

(1) Wang Baocun, June 13 and June 20, 1995, Op.Cit.,

الأخرى بما يمثل في إمكانية تعرضها لهجوم محتمل بما يمكن أن يأتي في شكل رد فعل يتمثل في الحق الشرعي للدفاع عن النفس، وأن استهداف الاتصالات وأنظمة المواصلات وخدمات الطوارئ والخدمات الحكومية يمكن أن يؤدي إلى الأضرار بالحياة والممتلكات.(1)

وذلك الى جانب التأثير النفسي على السكان بما يؤثر على درجة استقرار المجتمع مع انتشار استخدام تكنولوجيا الاتصال والمعلومات وزيادة الاعتماد عليها وإتاحتها أمام جميع المستخدمين دون تمييز بما يمكن أن يؤدي إلى استخدام الفضاء الإلكتروني كوسيلة من وسائل الصراع داخل الدولة Inte-State Conflict، حيث أصبح له دور في ممارسة المزيد من الضغط كونه ايضاً يعد وسيلة إعلام حرة يستخدمها الفرقاء السياسيين كساحة لتصفية الحسابات الشخصية.

والتعبيرعن مجموعه المصالح الفئوية الجزئية، مما يجعل الناس يشعرون بالعجز وعدم الثقة في مؤسسات الدولة والاحتماء بالولاءات التقليدية الأولية دون الانتماء للدولة القومية بما يشكل بداية استخدام الدين والقبيلة والعرق والمصالح الخاصة كدوافع من دوافع الصراع والتي يمكن إن تؤدي إلى تقويض سلطة الدولة وعدم استقرار المجتمع وكان لتكنولوجيا الاتصال والمعلومات دور في وجود أهداف جديدة ووسائل جديدة، ووفرت إمكانية التعرض للهجوم من خلال استخدام شبكات الاتصالات والمعلومات، مما أوجد نوعاً جديداً من الضرر يستخدمه العدو وذلك دون الحاجة للدخول الطبيعي والمادي لإقليم الدولة، وذلك لاعتماد الدول على الأنظمة الالكترونية بما يجعل من تلك الأنظمة هدفا للهجوم، وخاصة أن تلك الأنظمة تحمل طابعا مدنياً وعسكريا مزدوجا بما يجعل هناك خلطاً واضحاً بين ما هو مدني وما هو عسكري.

وتعد هجمات الفضاء الإلكتروني من احد أنواع النزاع المسلح ديناميكية والتي تختلف عن شكل النزاع التقليدي. فإحدى الفرضيات التي يمكن أن تحدث وقد تحدث بشكل غير مرئي أن تقوم القوات الخاصة لأي دولة بشن هجمات باستخدام الأسلحة الالكترونية في مهاجمة البنية التحتية المعلوماتية الخاصة بدولة أخرى.(2)

ويتيح الفضاء الإلكتروني في حالة نشوب الصراع إمكانية توسيع دائرة المشاركين بالعمل الهجومي، وكذلك إمكانية الوصول إلى أماكن بعيدة ، وتعدد أنماط استخدام الأسلحة عبر الفضاء الإلكتروني لشل الخدمة أو تدمير موقع ما أو سرقة المعلومات السرية، وتتميز تلك الأسلحة بسهولة الانتشار والقدرة على التأثير على الأهداف "الجاهزة إلكترونياً"، وبالبنية التحتية الحيوية ومؤسسات اقتصادية ومالية وسياسية وعسكرية (3). وجاءت تلك المظاهر لتبرز استخدامات غير سلمية للفضاء الالكتروني وما يمثلة ذلك من تهديد للأمن الالكتروني العالمي والبنية التحتية الكونية للمعلومات من

---

(1) Myriam Dunn, " Information Age Conflicts :A Study of the Information Revolution and a Changing Operating Environment", Center for Security Studies (CSS), ETH Zurich, Issue No. 64, 2002.

(2) Mark R. Shulman," Discrimination in the Laws of Information Warfare",School of Law Faculty Publications, Pace University,Columbia Journal of transnational Law ,1999,pp 937- 998 . (http://digitalcommons.pace.edu/lawfaculty/224).

(3) Martin C Libicki, "**Conquest in Cyberspace: National Security and Information Warfare**", New York, Cambridge University Press, 2007. pp 13 -323.

جانب كافة الفاعلين في مجتمع المعلومات العالمي، كالدول والمنظمات الإرهابية والأفراد وعناصر إجرامية وآخرين، وبما ينتج عن هذا الاستخدام أضرار وآثارمشابهه للهجمات التقليدية.

ويواجه الفضاء الإلكتروني عدداً من التحديات الذاتية والخارجية لعل أهمها ما يلي:

اولا :- تحديات زيادة الاستخدام والانتشار

إن العامل الأساسي وراء تدمير الشبكة هو عدم تحديث البنية التحتية الحالية بعد ما صارت قاصرة إمام استيعاب متطلبات التحميل المتزايد وأعداد المشتركين المتزايدة، وما يفرضه من تحديات أمام تحرك لمد سعة الإنترنت، وهناك نظريتان حول مستقبل الإنترنت الأولى اقل شعبية والثانية الأكثر تداولا النظرية الأولى تري أن الإنترنت بإمكانياتها المحدودة حاليا وتوسعاتها المنتظرة مستقبلا لا تتحمل ذلك التناقض مما قد يؤدي إلى انكماشها على نفسها وانهيارها بالتبعية، أما النظرية الثانية تعتمد فكرة التمدد الذاتي اللانهائي الذي يتبناه بعض الفلكيين بشان الكون ويرون أن الإنترنت أصلا مجتمع قابل للتمدد بطبعه وسبق أن تجاوز تنبؤات خطيرة بشان مستقبلة وتتضمن تلك التحديات الذاتية ١- الشبكة ٢,٠ والهجمات من جانب المستخدمين والزبائن ٢- هجمات تستهدف الرسائل ٣- شبكات "بوتنيتس" الموجهة لاستعباد الكومبيوترات والتحكم فيها كآلات طيّعة ٤- تهديدات تستهدف جميع الأجهزة الجوالة ٥- تهديدات تستهدف نظم التعريف بالهوية بالموجات الراديوية "RFID".[1]

ثانيا :- خطر الكوارث الطبيعية أو العرضية للكابلات البحرية

تعد الكابلات البحرية جزءاً هاماً من البنية التحتية الكونية للمعلومات: و الكابلات البحرية Submarine Cablesأو الخطوط البحرية عبارة عن كابلات توضع في أعماق البحار والمحيطات، لتوفير خدمة الاتصالات بين دول العالم عبر نقل البيانات، بما فيها الراديو والتلغراف والتلفزيون، والهاتف والإنترنت، وشبكات الكمبيوتر، وغيرها وذلك بعد إن كانت مقتصرة على نقل بيانات التلغراف. وشهدت عملية الربط بين أجزاء العالم المختلفة تطورا كبيرا، فمنذ عام ٢٠٠٥ أصبحت الكابلات البحرية تربط كل قارات العالم ما عدا مناطق القطب الجنوبي غير المأهولة، هذا على مجال الاتساع والانتشار أما على نطاق التقدم الفني فقد شهدت تطورا من الاعتماد على تقنية النحاس والرصاص والفولاذ، إلى تقنيات أخف وزنا وأصغر حجما، كالألياف البصرية،[2] والتي تتميز بسرعة نقل البيانات، وهذا ما تتطلبه شبكة الإنترنت وتطبيقاتها المختلفة وخصوصا التفاعلية منها والتي تستدعي نقل الصور والجرافيكس وملفات الأوديو والفيديو، وتتعرض تلك الكابلات إلى عدد من المشكلات التي تؤثر سلبا على أعمال الشبكة الدولية مما قد يسبب خسائر اقتصادية جسيمة ويهدد البنية التحتية بالضرر[3]

---

[1] **Emerging Cyber Threats Report for 2008.** Georgia Tech Information Security Center, October 2, 2007.(http://www.gtisc.gatech.edu/pdf/GTISC%20Cyber%20Threats%20Report.pdf)

[2] هي ألياف دقيقة ورفيعة للغاية وشفافة مصنوعة في العادة من الزجاج أو البلاستيك، وهي تقنية متقدمة للغاية، ومن أهم خصائصها : أولا: نسبة فقدان البيانات متدنية للغاية -وثانيا: سرعة فائقة في نقل البيانات، وأسرع بآلاف المرات من التقنيات القديمة المرتكزة على النحاس -وثالثا :مناعة ضد التداخل الكهرومغناطيسي ، ولا تصدر إشعاعات كهرومغناطيسية -و رابعا: وزن خفيف. أما المآخذ على هذه التقنية فأهمها: التكلفة العالية، وتحتاج إلى كم كبير من المرسلات البصرية والمستقبلات الغالية الثمن.

[3] هناك لجنة دولية لحماية الكابلات البحرية (International cable Protection Committee ) وهي تضم ٨٥ شركة عالمية في هذا المجال ويمكن الاطلاع حول اهداف اللجنة واعضائها ونشاطها من خلال موقعها على الإنترنت على الرابط : www.iscpc.org

وتعرض تلك الكابلات للضرر لا يقع في مياه المحيط العميقة وإنما بالقرب من الشواطئ، أما بسبب أنشطة الصيد البحرية، واستخدام مراسي السفن، أو كوارث طبيعة كالزلازل والبراكين أو ما قد تتعرض لخطر اعتداءات إرهابية أو خطر نشوب حرب بحرية، او في إطار منافسة اقتصادية ما بين شركات تكنولوجيا المعلومات والاتصال او انتهاء العمر الافتراضي لتلك الكابلات وضعف الصيانه.

وتعرضت دول الشرق الأوسط لانقطاع مفاجئ للانترنت في ١٩ ديسمبر ٢٠٠٨ تسبب في قطع خدمة الانترنت بنسبة ٨٠٪ في مصر و منطقة الشرق الاوسط [1] وكان قد حدث قطع سابق في ٣٠ يناير ٢٠٠٨ وذلك بسبب قطع في كابل بحري في البحر المتوسط مما أدى لتضرر شبكة الإنترنت في عدد من الدول الخليجية والعربية والهند مما عطل الحياة التكنولوجية وأصابها بالشلل، وقد حدث انقطاع لـ٥٠ كابلا في المحيط الاطلنطي خلال عام ٢٠٠٧ فقط، وحدث تعطل في باكستان في ٢٨ يونيو ٢٠٠٥، وفي ٣٠ من نوفمبر ٢٠٠٦ حدث خلل شبكة الإنترنت بالبحرين سببه خلل الكابل بين الهند وماليزيا، وأدى حدوث زلازل في جنوب شرق آسيا في ٢٧ ديسمبر ٢٠٠٦ إلى تعطل الاتصالات وقطع الكابلات البحرية. [2]

ثالثا :- القراصنة وتهديد امن الشبكة الدولية :

تشير الإحصائيات حول التأثير الاقتصادي للاستخدام الإجرامي لتكنولوجيا الاتصال والمعلومات بأنه يكلف الاقتصاد الدولي ما يقارب ٢٥٠ بليون دولار أمريكي سنويا وتشير التقديرات إلى إن تكلفة الفيروسات والديدان والرسائل المتطفلة وغيرها في تصاعد مستمر، وفي عام ٢٠٠٢ قدرت خسائر الولايات المتحدة بنحو ٤٥٥، ٨ بليون دولار، وقدرت وزارة العدل الأمريكية بان هناك ١٥٠ ألف شخص تأثروا بخسائر تجاوزت ٢١٥ مليون دولار، وفي سبتمبر ٢٠٠٣ أصدرت لجنة التجارة الفيدرالية الأمريكية تقريراً اقر بان هناك ٩، ٩ مليون مواطن أمريكي تعرضوا لتأثير هجمات الفضاء الإلكتروني مع متوسط خسارة ١٢٠ دولار لكل فرد وأصبحت الأعمال التي تعتمد على الإنترنت تتعرض للخسائر المالية المباشرة وغير المباشرة والإساءة للسمعة. [3]

وفي النصف الأول من عام ٢٠٠٥ شهد العالم ٢٣٧ مليون هجوم وفق شركة IBM، وقدرت الخسارة العالمية من هجمات الفضاء الإلكتروني للاقتصاد الدولي بـ ١٠٠ بليون دولار عام ٢٠٠٧، وأصبح الإنترنت خطرا بسبب الفيروسات وحلقات التجسس ووسائل الاحتيال الأخرى فقد تعرض نحو ربع المستخدمين لعمليات احتيال وبلغت الخسائر للمؤسسات والأفراد الناجمة عن هذه الهجمات نحو ٧ مليارات دولار خلال عامين، وقد أوقفت الشرطة النيوزيلندية فتى للاشتباه في انه سبب خللا في أكثر من مليون جهاز كمبيوتر بفيروس صممه بنفسه تمخض عن خسائر تجاوزت ٢٠ مليون دولار للمتضررين [4]

---

(1) جريدة الاهرام، ٢٠ ديسمبر ٢٠٠٨ .

(2) عادل عبد الصادق، " من قطع كابلات الانترنت عن الشرق الاوسط "، ملف الاهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية، جريدة الاهرام، العدد ١٦٠، ابريل ٢٠٠٨ ص ص ٤٥-٤٦ .

(3) تقرير شركة مكافي لأمن الشبكات الالكترونية والإنترنت، الحرب الباردة الالكترونية، ٢٩-١١-٢٠٠٧

(4) جريده الحياه، ١ ديسمبر ٢٠٠٧.

رابعا:- خطر التعرض للحرب الالكترونية في الفضاء الإلكتروني:

ظهر تنام في إدراك أخطار الهجمات الجديدة، فيما يمكن تسميته بالحرب الباردة الالكترونية، والتي أصبحت تمثل اكبر تهديد امني لاستقرار العالم وأسواقه المالية وحتى للبنية التحتية المدنية إضافة إلى الجهود الرامية لاكتشافه في مجالاته الفضائية ومـوارده الأساسية، التي تشن على أجهزة الكمبيوتر في العالم مما ينذر بتحوله إلى اكبر تهديد امني، وهناك ما يقرب من ١٢٠ دولة تطور أساليب استخدام الإنترنت كسلاح لاستهداف الأسواق المالية ونظم الكمبيوتر والخدمات الحكومية إضافة إلى الشبكات الالكترونية لتوزيع الكهرباء والغاز والماء.

وتختبر أجهزة الاستخبارات الدولية شبكات الدول الأخرى بصورة دورية بحثا عن ثغرات وتزداد أساليبها تطورا باستمرار،وشهد العديد من الدول التعرض للهجمات كان من بينها الولايات المتحدة والهند وألمانيا وفرنسا وبريطانيا عام ٢٠٠٧ بالإضافة إلى الهجوم على استونيا في مايو ٢٠٠٧، وفي الحرب الجورجية الروسية في ٢٠٠٨ وتطورت الهجمات الالكترونية من مجرد عمليات بحث بدافع الفضول في البدء الى عمليات جيدة التمويل والتنظيم من التجسس السياسي والعسكري والاقتصادي والتقني. وتم الكشف عن شبكة تجسس الكترونية تعمل في الصين تمكنت من اختراق١٢٩٥ جهاز كمبيوتر في١٠٣ دول بالاضافة الى مكتب الدلاي لاما وتعد الحادثة الاكبر في العالم من حيث عدد الدول التي تم اختراق شبكاتها واجهزتها منها وزارات الخارجية كل من ايران وبنجلاديش ولاتفيا واندونيسيا والفلبين وبروناي وتايلاند وبوتان.وتم اكتشاف اجهزة تنصت علي الكمبيوتر في سفارات كل من الهند وكوريا الجنوبية واندونيسيا وقبرص ومالطا وتايوان والبرتغال والمانيا وباكستان.[1]

خامسا :- استخدام الجماعات الإرهابية للفضاء الإلكتروني

يمثل الفضاء الإلكتروني عنصر جذب هام للجماعات الإرهابية على مختلف أشكالها وتنويعاتها الايدولوجية لما يتيحه من وسيلة إعلام دولية وسلاح في ذات الوقت يمكن استخدامه من قبل الأطراف المختلفة، ويعد تنظيم القاعدة أكثر الجماعات الإرهابية التي مثلت تهديداً حقيقياً لسلامة شبكة الإنترنت العالمية باستخدامه في الدعاية والتجنيد والتمويل وجمع المعلومات وتنسيق الهجمات المعادية لأميركا وحلفائها، ووسيلة لاستدعاء واستنفار مناصريها المنتشرين في دول شتى. كما تُسخّرها لاختراق المواقع الرقمية للكثير من المؤسسات المالية الدولية وسرقة ما فيها من وثائق ومعلومات وأموال أيضاً. وبشكل يظهر نوعا من الإرهاب الجديد العابر للقوميات.

[1] جريده الاهرام ٣٠ مارس ٢٠٠٩ وانظر ايضا

John Markoff,, Vast Spy System Loots Computers in 103 Countries , New York Times, 28-3-2009 (http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1&hpw)

## المطلب الثاني:

## الفضاء الإلكتروني كساحة للصراع والتنافس الدولي

يعد الصراع في الفضاء الإلكتروني نموذجاً آخر ذا طابع رقمي يعكس النزاعات التقليدية التي تخوضها الدول أو الحركات الراديكالية على خلفيات دينية أو عرقية أو إيديولوجية. ولأن الصراعات "الفعلية" تستعمل شتى أنواع أسلحة التدمير الاقتصادية والالكترونية والسياسية والإعلامية، فإنها لم تتوان عن استخدام الفضاء الإلكتروني، بما له من تأثير نفسيٍ ومعنويٍ وإعلامي، وشيئاً فشيئاً، زحفت جبهات القتال التقليدية لتصنع مجالا موازيا لها في الفضاء الإلكتروني"[1]

والصراع الالكتروني صراع فيه تدميرلا يصاحبة دماء وأشلاء بالضرورة، يتضمن التجسس والتسلل ثم النسف لكن لا دخان ولا أنقاض ولا غبار، ويتميز أطرافه بعدم الوضوح وتكون تداعياته خطيرة سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة ، للنيل من سلامة تلك المواقع ،وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت أيضا وتعلم كيفية استخدامها كما إن انتشار الفضاء الإلكتروني وسهولة الدخول اليه يمكن أن يوسع دائرة استهداف المواقع بالإضافة إلى زيادة عدد المهاجمين، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع ممتد يرتبط بطبيعته المختلفة ما بين طابع أيديولوجي وسياسي واقتصادي وإعلامي.

وما الصراع الالكتروني إلا صراع تحركه دوافع سياسية ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني وذلك بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية وبما يتضمن استخدام أسلحة وأدوات الكترونية من قبل فاعلين داخل المجتمع المعلوماتي أو من خلال التعاون ما بين قوى أخرى لتحقيق أهداف سياسية، وهناك صراع الكتروني بوجه أخر مرن عن طريق الصراع حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية. ويعد الصراع الالكتروني انعكاس للصراعات التي تدور على ارض الواقع وتكشف عن طبيعة الفاعلين وأنماط هذا الصراع، ويعد الصراع حالة سببها تعارض حقيقي أو متخيل للاحتياجات والقيم والمصالح. "[2],

ويمكن أن يدور الصراع داخليا أو خارجيا على مستوى الأفراد والدول أو ما بين الدول والمنظمات الإرهابية وغيرها من الأطراف ويساعد الصراع كمفهوم على تفسير الكثير من جوانب الحياة الاجتماعية، مثل الاختلاف الاجتماعي وتعارض المصالح والحروب بين الأفراد والجماعات أو المنظماتو من الناحية السياسية يمكن أن يشير الصراع إلى الحروب أو الثورات أو النضالات، والتي قد تنطوي على استعمال القوة كما هو الحال في الصراع المسلح .

وتؤدي الصراعات في بيئات اجتماعية إلى التوترات عند عدم وجود حل سليم لها أو ترتيب للتعامل معها. والتعريف الشائع للصراع: "عندما يتصور طرفان أو أكثر تعارض الأهداف ويسعيان إلى إضعاف

---

(1) عادل عبد الصادق " هل يمثل الارهاب الالكتروني شكلا جديدا من أشكال الصراع الدولي " ملف الاهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد ١٥٦- ديسمبر ٢٠٠٧.

(2) Athina Karatzogianni,(ed), "Cyber-Conflict and Global Politics'", Routledge and Taylor & Francis Group. , 11th September 2008, pp. 240- 272 .

قدرات الآخر للوصول للهدف."، و في علم الاجتماع و علم الأحياء، يدل مصطلح نظرية الصراع أو نظرية النزاع Conflict Theory على نظرية تقول بأن المجتمعات أو التنظيمات بشكل عام تعمل من خلال صراع أعضائها و مشاركيها المستمر للحصول على منافع أكثر، و هذا ما يسهم بشكل أساسي في التغير الاجتماعي كحالة التغيرات السياسية والثورات والصراعات الطبقية خاصة في أيديولوجيات مثل الاشتراكية والشيوعية.

ويُعد مفهوم الصراع أحد أبرز المفاهيم المتداولة التي طفت على السطح بعد انتهاء الحرب الباردة، وتأخذ الصراعات شكل تطور المجتمع الدولي حيث تكون تعبيرا عن الواقع الاجتماعي والتكنولوجي، ففي عصر الثورة المعلوماتية يأخذ الصراع أدوات جديدة للتعبير وما ينعكس على تداعياته وأطرافه داخل مجتمع المعلومات الدولي، ومثل ظهور الفضاء الإلكتروني ساحة جديدة إما لنقل الصراعات من خلاله أو استخدامه نفسه كوسيلة من وسائل الصراع والذي يعد امتدادا طبيعيا للصراع بشكله المادي.[1]

والصراع الالكتروني هو ذلك الصراع الذي يمكن أن ينشب في بيئة يكون وسيطها الفضاء الإلكتروني حيث يشهد حركة التفاعلات بين مختلف أنواع الصراعات والتي قد تنشب من كل أنواع البيئات الأخرى غير المتصلة بالفضاء الإلكتروني وإنما تؤثر فيه كالنزاعات بين الأفراد والصراع ذو الطابع القانوني والتجاري أو الصناعي ويمتد ليشمل كافة مجالات الحياة، وهناك صراع يأخذ طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع، والتنافس للسيطرة على سوق استضافة المواقع عبر الخوادم التقنية والتوجه أحيانا للتحكم بالمعلومات وطرق تبادلها عبر التحكم بالحلول التقنية واحتكارها لتكون وسيلة التحكم بمصائر المستخدمين وأداة السيطرة الفعلية، وذلك مع غياب المركزية وغياب السلطة التحكمية التي تنظم عمل هذا المجال الحيوي والذي يتعرض لاعتداء عسكري أو إرهابي بدون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السيادية بل سيكون هجوماً في الفضاء الإلكتروني يشنه قراصنة الكمبيوتر وتدمير المواقع والتجسس وإقامة مراكز لمواقع إرهابية، والقدرة على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر.

وقد تطورت الهجمات الالكترونية من مجرد عمليات بحث بدافع الفضول في البدء، إلى عمليات جيدة التمويل والتنظيم من التجسس السياسي والعسكري والاقتصادي والتقني. وأصبح الفضاء الإلكتروني مجالا للصراع والتنافس ويستخدمه الفاعلون فيه من الدول أو من غير الدول للتعبئة والحشد والتنظيم والدعاية ويستخدمها أيضا المعارضة ضد النظم السياسية أو نشطاء الإرهاب أو الجريمة، وهناك صعوبة الفصل ما بين النشاط الذي يتعلق بالاستخبارات وجمع المعلومات و حرب الفضاء الإلكتروني و الاستخدام السياسي له في الصراع، وخاصة مع يمثله من بيئة مثالية لعمل

---

[1] Bonnie N Adkins, The Spectrum of Cyber Conflict from Hacking to Information Warfare: What Is Law Enforcement's Role? ,**Op.Cit.**, pp.56-89.

الجماعات المختلفة والقدرة على تشكيل شبكة عالمية بدون سيطرة مباشرة بالإضافة إلى رخص تكلفة وسهولة الاتصال وضعف الرقابة التقليدية عليه، ومثلت تلك الخصائص عنصر جذب هام لاستخدامها وتوظيفها لتحقيق الأهداف السياسية، حيث أصبح الفضاء الإلكتروني ساحة لنقل الصراعات وأشكالها وتتراوح من حرب الأفكار والأفكار المضادة إلى التوظيف العملي للصراع بما قد ينطوي عليه من عمل عنيف.

ويكون للبيئة المحلية والسياق الدولي للفضاء الالكتروني تأثير كبير على بروز الصراعات وفي دعم الهيكل التنظيمي والاتصالي داخل الجماعات كما أن له دوراً في عمليات التجنيد والحشد والتعبئة والتمويل ووضع التكتيكات، و تشكيل أولويات القضايا الإستراتيجية وتأثيرها على الهوية وعلى هيكل الفرص السياسية، وفي تفعيل دور النشطاء السياسيين، وظهرت صراعات الكترونيه ذات طابع ديني أو عرقي وكذلك الصراعات ذات الطابع العنصري والصراع الذي يظهر في شكل ظاهرة الارهاب الالكتروني.[1] و كان للفضاء الالكتروني دورا في حل الصراعات و المصالحة، وأصبح وسيطا في الصراع عن طريق قدرته على بناء الهويات الاجتماعية والعلاقات الاجتماعية، والقدرة على التحكم في المعلومات والأحداث ، بالاضافة لدور الفضاء الإلكتروني كوسيلة إعلام وتأثيرها على البعد الاستراتيجي والتكتيكي للصراع. ويمكن للصراع الالكتروني أن يحدث داخل أو عبر كل جهاز عام أو خاص وتمدد داخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول، ويؤثر ذلك في امتداد مجال الصراع فيه وبما يؤثرعلى تفاقم تداعياته أو أثاره حيث يتم الاستخدام المتعدد للصراع من وجهه نظر الاقتصاد والسياسة والاجتماع أو الأمن أو الثقافة، فهناك الصراع ضد العولمة والحركات المعادية للرأسمالية حيث تتم المطالبة ببرنامج بديل للإصلاح .

وهناك الحركات المناهضة للحرب حيث تتركز دعوتها على إنهاء حالة الحرب والدعوة إلى إحلال السلام وان طبيعة الحرب غير عادلة وما يترتب عليها من ماسي للبشرية، وهناك أيضا صراع تقوده الحركات الاجتماعية الجديدة والتي تتنوع أهدافها في مجال العمل المدني العام من حركات تهتم بتمكين المرآة إلى حقوق الطفل أو حقوق الإنسان أو جماعات حماية البيئة وغيرها وتهدف الحركات الاجتماعية إلى استخدام الفضاء الإلكتروني من اجل التأثير في الرأي العام وتعبئة وحشد الجمهور .

وهناك الصراع السياسي الذي يدور ما بين الحكومات أو النظم الحاكمة والجهات المعارضة لها أو الجماعات العرقية والدينية المهمشة مثل حالة استخدام الفضاء الإلكتروني في الصراع العربي الإسرائيلي أو ما بين باكستان والهند أو ما بين الصين والولايات المتحدة أو ما بين الصين وتايوان أو كوسوفا أو غيرها من مناطق الصراعات ذات الطبيعة الاجتماعية الممتدة.

وتصبح الدولة ضحية إذا ما تم مهاجمه نظم شبكاتها الالكترونية وتأثيرهذا الهجوم على المؤسسات المالية والمصرفية والتحكم في الطيران المدني والنظم المالية، بدون معرفه من ورائه وكيفية نجاحه وطرق تنفيذه وأطرافه الحقيقيه، مما يجعله قضية متشابكة وتأتي عملية الاستجابة للهجمات وعملية

---

[1] عادل عبد الصادق " هل يمثل الارهاب الالكتروني شكلا جديدا من أشكال الصراع الدولي"، مرجع سابق ذكره .

رد الفعل مع ضعف إجراءات الوقاية ضد التعرض لمثل تلك الهجمات، و التي يمكن أن يتم شنها عبر الفضاء الالكتروني والشبكات، أو من خلال استخدام الهجوم العسكري التقليدي، وللحصول على تأييد دولي للإجراءات الوقائية السلبية تكون هناك حاجة ملحة إلى تقديم الدليل أو إثبات تورط طرف ما في مثل هذا الهجوم (والذي يكون من الصعب التأكد بشأنه ) بما يشكل ضمانه لوجود إجماع دولي للتعاون في المكافحة أو الحرب ضد طرف أخر أو فرض عقوبات دولية ما، حيث تكون الدول معرضة لانتهاك لسيادتها وأمنها الداخلي.

وما يكون له من انعكاس على المستوى الدولي مع عولمة الشبكات والإنترنت وارتباطها بالاقتصاد العالمي قاطبة، ومن ثم فان الدولة الضحية يتم إصابتها دون النظر إلى حدودها أو نطاقها الجغرافي بل ومن الممكن أن يكون الهجوم من الداخل من قبل عملاء دولة ما أو عملاء مقيمين في دولة أخرى يقومون بشن هجمات من خلال نطاقها الجغرافي دون تورط تلك الدولة في دعم مباشر لها وما يتعلق بإشكالية المسؤولية القانونية عن تلك الهجمات ويواجهه الفضاء الإلكتروني بتحديات تتعلق بدورة الاستراتيجي والحيوي في النظام الدولي منها ما يتعلق بعوامل ذاتية وأخرى خارجية وأخري ترتبط بالتفاعل ما بين البعد الخارجي والطبيعة الذاتية له ومن أهم تلك التحديات الإرهاب الإلكتروني لما مثله من تحديات واشكاليات للمجتمع الدولي تمثلت في: [1]أولا :ارتباط العالم المتزايد بالإنترنت اقتصاديا وأمنيا عمل على زيادة التعرض لخطر هجمات إرهابية الكترونية مع العولمة الاتصالية والاقتصادية. ثانيا: استخدام الجماعات الإرهابية للفضاء الالكتروني لتحقيق أهدافها وتقويض سلطة الدولة والتأثير في الرأي العام وتهديد شرعية النظم السياسية الحاكمة. ثالثا: فرض انسحاب الدولة من قطاعات إستراتيجية لصالح القطاع الخاص كذلك تحديات أمنية متزايدة.، رابعا: تأثير الإرهاب الإلكتروني على حرية الرأي والتعبير عبر الإنترنت كقيم ديمقراطية وكيفية الموازنة بين دور الدولة كميكانيزم للضبط الاجتماعي وبين إتاحة الإنترنت كخدمة. خامسا: عدم وجود اتفاق عالمي حول التعريف القانوني للسلوك الإرهابي مما ينعكس على مشروعية ممارسة الإرهاب الإلكتروني. سادسا: تداخل الإرهاب الإلكتروني مع غيره من المفاهيم كالجريمة الإلكترونية والمنظمة والاحتيال والتجسس وقرصنة المعلومات وحرب المعلومات وغيرها بما فرض إشكالية تحديد المعاملة القانونية الواضحة سابعا :عنصر المباغتة الذي يتميز به الإرهاب الإلكتروني وخاصة في بعده الرقمي مما يجعلة تحديا أمنيا يضع الطرف الأخير في موقف ضعيف حيث يقتصر دوره في تلك الحالة علي رد الفعل مع إصابة الإجراءات الوقائية في مقتل. ثامنا تطرح مسالة تعدد الفاعلين في استخدام الإرهاب عبر الإنترنت قضية المسئولية القانونية خاصة أن استخدامه قد لا يقتصر على الدول بل قد تستخدمة الجماعات والأفراد، وهو ما يخرج عن الالتزامات القانونية الدولية. تاسعا: يضفي البعد الدولي للظاهرة تعقيدا في شأن المواجهة الدولية خاصة مع عدم وجود إطار قانوني دولي واضح حتى الان لتناول تلك الظاهرة المستحدثة والحاجة إلي قانون دولي جديد أو محاولة عقد اتفاقيات مكملة للاتفاقيات الدولية أو تفعيل اتفاقيات أخري قائمة.

---

[1] عادل عبد الصادق " هل يمثل الارهاب الالكتروني شكلا جديدا من أشكال الصراع الدولي، مرجع سابق ذكرة، ص ص ١٥-١٦.

## المطلب الثالث:

## هجمات الإرهاب الإلكتروني: حرب غير متماثلة وحرب غير تقليدية

اولا : الفضاء الالكتروني و الحرب غير المتماثلة

ظهر مفهوم الحرب غير المتماثلة "a symmetrical War" والتي تعبر عن "محاولة طرف يعادي الدولة القومية أن يلتف من حول قوتها ويستغل نقط ضعفها معتمدا على وسائل تختلف بطريقة كاملة عن نوع العمليات التي يمكن توقعها وعدم التماثل يعني أن يستعمل العدو طاقة الحرب النفسية وما يصاحبها من شحنات الصدمة والعجز كي ينتزع في يده زمام المبادرة وحرية الحركة والإرادة، وأسلوب يستخدم وسائل مستحدثة وتكتيكات غير تقليدية وأسلحة وتكنولوجيات جري التوصل إليها وتطبيقها على كل مستويات الحرب من الإستراتيجية إلى التخطيط إلى العمليات، ومن ثم فان الحرب غير المتماثلة هي شكل غير تقليدي من الحرب حيث يستخدم الطرفان أسلحة غير متماثلة ويمتاز العدو بإرادة قوية وإصرار على تحقيق الأهداف [1] وتعد الحرب غير المتماثلة هي مزيج العلاقة ما بين التكنولوجيا والحرب وهي نوع من الحروب يحاول أن يحُد ويُقوّض من عناصر القوة لدى العدو ومن استغلال نقاط ضعفه بطريقة مُبدعة جديدة تُحقق الانتصار الأخلاقي والمعنوي. وتكون معارك هذه الحرب في الجهة الخلفية للعدو، باستخدام العمليات الحربية النفسية ووسائل الإعلام وعن طريق الإبداع الخلاّق للقدرات المتوفرة والتشتت والاتصال وتلاقي المعركة الفاصلة، من أجل شل قدرات العدو وعزمه وإرادته. ويمثل نمط الحرب غير المتماثلة عودة إلى طُرق الحرب قبل ظهور وصعود مفهوم "الدولة"، و حيث تتحوّل عناصر القوة إلى ضعف ويُعاد صياغة معنى النصر والهزيمة. وتتحول بذلك طبيعة المعركة ، وتصبح الأهداف ضرب مراكز القوة الاجتماعية- الاقتصادية والسياسية- الثقافية إضافة إلى العسكرية.[2]

وتتميز الحروب الجديدة بأنها ذات أبعاد ثقافية وليست لأسباب جيوسياسية أو تنازع حول السيادة الإقليمية بالضرورة ،و تتميزباختلافها عن الحروب النظامية القديمة و حرب المناورات والجبهات و حروب العصابات، وأصبحت تلك الحروب الجديدة تتوخى الكسب السياسي للسكان عبر كسب العقول والقلوب، وزعزعة الاستقرار وزرع الخوف والحقد والسيطرة على السكان عبر إزالة كل هوية مختلفة، فهي حرب ضد الغريب وضد المخالف من داخل الجماعة نفسها ، ويعد طرد السكان والقتل الجماعي والتهجير القسري جزءاً من تقنيات الترهيب السياسي الجديد. وبات ضرب المدنيين والحصار والتعذيب والقتل الكيفي وتدمير المعالم الحضارية التاريخية والبنية التحتية من المباحات في تلك الحروب، وكانت الحروب القديمة تعتمد على تشكيلات عسكرية ذات تنظيم عمودي أو قد تشمل وحدات منشقة عن الجيش وزعماء ميلشيا ومرتزقة ومافيات إجرامية واستخدام حتى جماعات إرهابية وهي ذات تنظيم لا مركزي تنشط بمزيج من المواجهة والتعاون بين وحدات الجيش المختلفة عبر وسائل

---

([1]) محمد عبد السلام ،"الحرب غير المتماثلة بين الولايات المتحدة و القاعدة "، مجلة السياسة الدولية ، العدد ١٤٧ يناير ٢٠٠٢

(2) David J. Lonsdale, **The Nature of War in the Information Age: Clausewitzian Future.** New York, Frank Cass, 2004. p 269.

الاتصال الحديثة.[1] وعملت الثورة التكنولوجية على إعادة التفكير في حركية وديناميكية الصراع. وظهر ما يعرف بـ "عصر القوة النسبية" التي يعني بها عجز القوة العسكرية عن تأمين الأهداف السياسية المترتبة عليها، مما يخلف آثارا إستراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي. ، وتغير"براديم" الحرب جذريا بانتقاله من نسق "الحروب الصناعية بين الدول" إلى نسق "الحرب في وسط الشعوب". ففي الحروب القديمة كان الغرض هو تدمير الخصم، إما باحتلال أرضه أو الاستيلاء على موارده، بينما أصبح في الحرب الجديدة هو التحكم في إرادته وخياراته، ومن ثم كان الدور المحوري للشعوب في هذا الصنف الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في البلد الذي يشن الحرب، أو بالرأي العام الإقليمي والدولي. فأهداف الحرب هنا أصبحت أقل مادية، يؤدي فيها العامل النفسي والدعائي دورا محوريا، وسببه تنامي التغطية الإخبارية السمعية البصرية المباشرة للأحداث لحظة وقوعها.

وإذا كانت الجيوش النظامية تسعى، باستغلال تفوقها التقني العسكري ـ الإعلامي الكاسح، لحسم حرب نظيفة سريعة تجنب السكان فظائع وآلام المواجهة، فان إستراتيجية الشبكات المسلحة المقاومة لها هي الاستخدام المعاكس لهذه الميزات التقنية، بالتسلل إلى وسط السكان والاحتماء بهم وبالتالي تحويلهم إلى أرضية مواجهة ومن ثم توجيه سلاح الصورة إلى مآسي الحرب وجرائمها الإنسانية.

وفي هذا المشهد تمحي الفروق التقليدية بين الحرب والسلم، في الوقت الذي يغدو فيه الصدام السمة الغالبة على الوضع الاستراتيجي الدولي، وان كان نادرا ما يتطور إلى حالة مواجهة مسلحة للوعي المتزايد بعدم نجاعه الحسم العسكري في إطفاء بؤر التوتر القائمة. و العلاقة غير المسبوقة القائمة بين التطرف ذي الخلفيات الدينية أو القومية وأسلحة الدمار الشامل الرخيصة وسهلة الإنتاج وبدأت عملية إعادة التفكير في الردع القائم على التوازن السلبي المفضي إلى العجز والجمود. وظهر اتجاه للمزج بين عاملي التنافس والتعاون، باللجوء إلى إستراتيجية مواجهة متدرجة تؤدي إلى إنهاك الخصم للتغلب عليه والذي أصبح غير ملائم للوضع الدولي مع بداية ظهور قوى صاعدة وظهور مشاكل عالمية تهم الأمن الإنساني المشترك[2] وأصبحت الحروب الجديدة هي نتاج ثورة في وسائل الاتصال وثورة المعلومات وأيضا ثورة في العلاقات الاجتماعية للحرب، واكتسبت الحروب الجديدة خصائصها كذلك من فراغ السلطة المميز للفترة الانتقالية التي ابتدأت بنهاية الحرب البادرة، وانهيار الأيدلوجيات وتفكك الوحدات السياسية ذات الطابع القومي وانفتاح العالم على بعضة فيما عرف بالعولمة والتي عملت على تكثيف درجة التكامل والاعتمادية بين دول العالم وزادت ثورة المعلومات من التفاعل والتجانس بالإضافة إلى تفتته وتنوعه وبرزت هويات من داخل الدولة تريد التعبير عن مصالحها مما زاد من حجم المطالب أمام الدولة، وأصبحت عاجزة في مواجهه تلك المطالب مما جعلها عرضة للتمرد عليها وعلى احتكارها لاستخدام القوة المشروع . وجاء هذا التآكل لقوة الدولة من جانب السياق الدولي و المحلي، وضعفت

(1) Lawrence T. Greenberg &, Seymour E. Goodman &, Kevin J. Soo Hoo," **Information Warfare and International Law**", National Defense University Press, 1998.
see at (www.iwar.org.uk/law/resources/iwlaw/iwilindex.htm - 19k)

(2) جريدة الشرق الاوسط ٣٠-١١-٢٠٠٧

قدرة الدولة على استخدام قواتها المسلحة انفراديا وبات تنظيم القوات المسلحة متعددة القوميات ،وبرزت ظاهرة خصخصة الأمن وشركات الأمن الخاصة التي يكون لها دور في الحروب - شركة بلاك ووتر في العراق- ، ومع تآكل شرعية الدولة في مرحلة ما بعد الحرب البادرة اندلع العنف الجديد المتمثل في ظهور الحرب الجديدة أوالإرهاب الجديد مزيلا الفروق بين المدنيين والمنشآت .

وقد كان اقتصاد الحرب القديمة يقوم على التنظيم المركزي الوطني للموارد، أما اقتصاد الحرب الجديدة فهو نقيض ذلك انه لا مركزي تماما يعتمد على الموارد الخارجية وعلى التمويل الذاتي عبر الاعتماد على النهب والسلب وأحيانا السوق السوداء ويعتمد هذه الاقتصاد على شبكات الضرائب وجذب مهاجرين الشتات والمتاجرة بالسلاح وتهريب النفط، ويتم الحفاظ على هذه الموارد عبر قوة السلاح ويعبر هذا الاقتصاد الحدود الدولية[1] وكانت إستراتيجية المتحاربين تلتقي في هدف موحد هو زرع الخوف ويتعاونون في خلق مناخ انعدام الأمن وهناك حالات تعاون بين المتحاربين تحقيقا لمآرب عسكرية واقتصادية وقد تهدف الحرب لدفع النمو الاقتصادي عبر تنشيط الصناعات العسكرية.

ثانيا : التحول من الحرب التقليدية الى غير التقليدية

في الحرب التقليدية تكون هناك تحديات للقوه من حيث الكم والكيف وتكون هناك حالة إعلان للحرب مسبقا، أما في الحرب غير التقليدية فان التحديات تتركز في كونها عوامل نفوذ، وتكون هجماتها استباقي من دون سابق إنذار، وتكون ساحة المعركة في الحرب التقليدية محددة زمانيا وجغرافيا وفي أطرافها، أما الحرب الغير تقليدية فإنها غير محدده المجال أو المدى وتكون أهدافها غير مأمونة بخلاف الحرب التقليدية التي تكون أهدافها محدده كميا، حيث تكون القوات المستخدمة في الحرب التقليدية قوات نظامية. أما في غير التقليدية فتكون قواتها غير معروفه وليست محدده في دوله سواء أكانت هدفا للحرب أو مشاركا فيها حيث لا تصبح بالضرورة الدولة هي الهدف، وتتميز الحرب التقليدية بأنها تشكل تحديا عسكريا فقط في حين تمثل الحرب غير التقليدية متعددة الأوجه ومتشابكة مع غيرها ومن ثم تكون تفاعلاتها كبيرة بخلاف الحرب التقليدية التي تكون تفاعلاتها محدودة، وفي الحرب التقليدية تكون هناك تحديات للقوه من حيث الكم والكيف وتكون هناك حالة إعلان للحرب مسبقا.[2] أما في الحرب غير التقليدية فان التحديات تتركز في كونها عوامل نفوذ، وتكون هجماتها استباقي من دون سابق إنذار، وتكون ساحة المعركة في الحرب التقليدية محددة زمانيا وجغرافيا وفي أطرافها، أما الحرب الغير تقليدية فإنها غير محدده المجال أو المدى وتكون أهدافها غير مأمونة بخلاف الحرب التقليدية التي تكون أهدافها محدده كميا، وتكون القوات المستخدمة في الحرب التقليدية قوات نظامية.أما في غير التقليدية فتكون قواتها غير معروفه وليست محدده في دوله سواء أكانت هدفا للحرب أو مشاركا فيها حيث لا تصبح بالضرورة الدولة هي الهدف، وتتميز الحرب التقليدية بأنها تشكل تحديا عسكريا فقط في حين تمثل الحرب الغير تقليدية

---

(1) جريدة الحياه اللندنية ، ١١-١١-٢٠٠٧

(2) John Borland, "**Analyzing the Threat of Cyberterrorism,**" **TechWeb: The Business Technology Network,** September 25, 1998, available online at http://www.techweb.com/wire/story/TWB19980923S0016) (accessed May 25, 200٨).

متعددة الأوجه ومتشابكة مع غيرها ومن ثم تكون تفاعلاتها كبيرة بخلاف الحرب التقليدية التي تكون تفاعلاتها محدودة، كما أن الحرب المعلوماتية تصبح متشابكة مع غيرها من الحرب الاعلاميه وحرب الشبكات والاتصالات والحرب السياسية والسيكولوجية والحرب التكنولوجية والارهاب[1]

وقام "كيفين كولمان Kevin Coleman" في دراسته بعنوان "تحديات الحرب غير التقليدية نظرة للأمام ونظرة للخلف "[2] بتحديد ١٤ نوعا من الحروب غير التقليدية كان هناك مالا يقل عن ستة أنواع ترتبط ارتباطا مباشرا بالإرهاب الالكتروني وهي حرب المعلومات والحرب الإعلامية وحرب الشبكات والاتصالات والحرب السياسية والحرب السيكولوجية والحرب التكنولوجية وبالطبع الإرهاب، في حين يرتبط الإرهاب الالكتروني بالأنواع الأخرى بطريقة غير مباشرة. وقام كولمان في دراستة عن "الحرب العالمية الثالثة هل بدأت حرب الفضاء الالكتروني" بتحديد خصائص الأسلحة الالكترونية وأضرارها وعملية تطويرها وتنفيذها مع الاشارة الى نموذج استونيا وترسانة الاسلحة الالكترونية ، وقام كولمان في تلك الدراسة بتطبيق معايير كمية على هذا النوع الجديد من الصراع حيث ربط بين الإرهاب الالكتروني والحرب الالكترونية والحرب غير التقليدية ، وأنها مرشحه للزيادة في غضون السنوات القادمة، وقد قام" كيفين كولمان Kevin Coleman" بعمل مصفوفة عبر فيها عن تحليل كمي للخطر يتراوح من الدرجة (1) إلى الدرجة (5) من خطر منخفض إلى خطر مرتفع ومستندا على دراسة الدوافع والإمكانيات لكل خطر من أخطار الحرب غير التقليدية، وقام بتقسيمها إلى الخطر الحالي والخطر المتوقع في المدى القصير وفي المدى الطويل وتداعياتها في الوقت الحالي والمدى القصير والطويل وكذلك قام بقياس القدرة على الدفاع ضد تلك الأخطار ودرجة التغير في الخطر.[3] وأوضحت دراسة كولمان أن كل ما يرتبط بالخطر الحالي يتركز في الحرب الشبكية والاتصالات والحرب التكنولوجية والحرب على الإرهاب والحرب القذرة والمخدرات والجريمة المنظمة حيث وصلت إلى درجة عاليه من التهديد (4) وكذلك الحرب المالية والإعلامية والمعلوماتية حيث وصلت على(3).أما عن التهديدات في الأجل القصير فحصلت تهديدات الحرب التكنولوجية والحرب على الإرهاب على أعلى درجة من الخطورة هي الدرجة (5) وجاءت التهديدات الخاصة بالمساعدة الاقتصادية والصراع المالي وحرب المعلوماتية ووسائل الإعلام وحرب الشبكات والاتصالات في الدرجة (4). أما في الأجل الطويل فإن تهديدات الحرب الشبكية والاتصالات والحرب على الإرهاب والحرب التكنولوجية ستصل إلى ذروتها (5)، في حين تأتي اكبر انعكاسات تلك التهديدات من الإرهاب الالكتروني والاتصالات في الوقت الحالي ويأتي بعدة الحرب التكنولوجية والإرهاب، أما عن التداعيات في الأجل القصير فإنها ستصل إلى ذروتها في الحرب الشبكية والاتصالات والإرهاب (5) ويأتي بعدة الحرب التكنولوجية والمالية، أما في الأجل الطويل فتصل تلك التهديدات إلى ذروتها وهي خطر الإرهاب والحرب التكنولوجية والإرهاب الالكتروني .

---

(1) Kevin Coleman , **The Challenge of Unrestricted Warfare - A Look Back and a Look Ahead,** Articles , www.directionsmag.com, Jan 11, 2006.

(2) ____________ , Op.Cit

(3) Kevin G. Coleman, **The world war 111,A Cyber War has begun, Cyber Warfare, The Technolytics Institute,** September 2007(http://www.technolytics.com/Technolytics_Cyber_War.pdf)

## المبحث الثاني:
## الإرهاب الإلكتروني
## كشكل جديد من أشكال الصراع الدولي

**يتناول هذا المبحث مظاهر صراع جديدة وباليات جديدة وفاعلين جدد وعلى درجة كبيرة من التنوع ما بين دور الحكومات والدول الى دور الافراد والجماعات الارهابية كما يتم تناول في هذا المبحث نماذج من ذلك الاستخدام حيث يتم عرض نموذج لاستخدام الدول ونموذج اخر لاستخدام الجماعات والافراد ويتم عرض ذلك من خلال تناول الباحث لثلاثة مطالب اولها الفضاء الالكتروني وأجهزة الاستخبارات الدولية ، واما المطلب الثاني فيتناول :استخدام الجماعات الإرهابية للفضاء الالكتروني ، ويتعلق المطلب الثالث :تنظيم القاعدة واستخدام الفضاء الالكتروني**

### المطلب الاول:
### الفضاء الإلكتروني وأجهزة الاستخبارات الدولية

أخذ الاهتمام العالمي بالبعد الأمني لشبكة الإنترنت يتزايد بعد إحداث ١١ سبتمبر٢٠٠١ والحملة الأمريكية على الإرهاب وما مثله ذلك من تحديات جديدة لأنظمة الحكم في العالم ، وكان نجاح تنظيم القاعدة في استخدامه للانترنت كاشفا من ناحية لقدرة الفاعلين من غير الدول سواء أكانوا جماعات أو أفراد على التحكم في المعطيات التكنولوجية ومن ناحية أخرى فجر الطابع الاستخباراتي لشبكة الإنترنت الذي طالما حاولت الدول الكبرى اخفاءه، حيث تمتلك الدول الفرص الأكبر في استخدم الفضاء الإلكتروني بما تملكه من قدرات فنية ومالية مقارنه بالجماعات الإرهابية التي نجحت في استخدامه هي الأخرى، حيث تمتلك الدول أجهزة استخباراتية قوية وخاصة الدول المتقدمة في تكنولوجيا الاتصال والمعلومات فضلا عن التقدم في مجالات التجسس بالأقمار الصناعية والموجات والاتصالات السلكية واللاسلكية.

أولا : الإنترنت و ثورة الاستخبارات

تقدم الإنترنت سيلا هائلا من المعلومات المتدفقة حول دول العالم وهي تلك المعلومات التي لا تقتصر على وجهة النظر الرسمية بل تتعداها إلى دور الأفراد في إنتاج المعلومات والترويج لها عبر الإنترنت ووجود كم هائل من التحليلات الصحفية والسياسية فضلا عن التقارير الاقتصادية وتعبيركافة التيارات السياسية والفكرية والدينية عن نفسها من خلال الإنترنت ووجود الخرائط الفضائية للأرض على الإنترنت بما فيها المنشات المدنية الحيوية والعسكرية وشكل ذلك ثورة معلوماتية طالما عكفت أجهزة الاستخبارات في العالم على الحصول عليها مع إمكانيات البحث الهائلة لدى محركات _مثل جوجل أو ياهو_ لديها القدرة على تصنيف المعلومات وتبويبها وسهولة الوصول إلى موضع البحث.

ومع هذا الخضم الهائل من المعلومات ظهر الدافع لدي العديد من دول العالم لاستخداماته السلمية والأخرى المخابراتية حيث تعتبر الأخيرة أداة سلطة الدولة على المعلومات وأحد فنون الحكم القائمة على

معرفة الأصدقاء والأعداء فهي أداة تحمل عده تناقضات حيث يتم فيها استخدام الألفاظ والصور والتقديرات والإيماءات والتحريض وفيها الحقائق والأكاذيب، ولان المخابرات هي أداة غير مادية فهي لا تجرح ولكنها تسبب في إلحاق خسائر مادية ونفسية ، وتتكون المخابرات من أربعه مكونات أساسية هي جمع المعلومات والاستخبار المضاد والتحليل والتحرك المستتر.[1] وأثرت ثورة المعلومات والاتصالات في منتج وطبيعة وأدوات عمل الأجهزة ونوعية المنتج والسياسة الاستخباراتية ، حيث كان التأثير يتعلق بمحورين أو معادلتين يتعلق الأول بنوعية منتج الاستخبارات التي تتوقف على جمع المعلومات ثم معالجتها وتحليلها ثم يتم بعد ذلك استغلالها ، أما المحور الثاني فيتعلق بالسياسة الاستخبارتية والتي تتم من خلال نوعية منتج الاستخبارات ومدى تاثيرة على إدراك وسلوك وخيارات الدولة لتخرج في شكل سلوك وخطة منضبطة لتؤثر فيما بعد على مستهلك السياسة والرأي العام وصانعي القرار.[2] وكذلك التعاون فيما بين أجهزة الاستخبارات داخل الدولة أو بالتعاون مع غيرها من الدول للتشارك في تعميم وتبادل المعلومات، ولم تعد مسالة استقطاب المعلومات أمرا معقدا بل صار أسهل من السابق فبعد أن كان العميل شخصا يتوجب تجنيده بشكل مباشر أصبح العميل يبدو جاهزا ومتصلا وبطريقة سهلة ومستترة، ومكن الإنترنت العميل من أن يرى نفسه مسموعا لأول مرة في حياته فيجد من يتحاور معه بشكل يمنحه ثقة كبيرة في نفسه ويخرجه من بيئته المحيطة بمشاكلها وتعقيداتها إلى عالم أرحب وهوية وانتماء من اختياره هو وليست مفروضة علية ، ويعد عملاء الإنترنت من أهم الركائز الإعلامية لأجهزة المخابرات الإسرائيلية والأمريكية من خلال تنشيط العمل الاستخباراتي البشري .[3]

ثانيا: بيئة جيده واستخدام متعدد

يوفر الفضاء الالكتروني بيئة يتم فيها شن الحرب النفسية ونشر معلومات وبيانات مضللة أو التحريض على الكراهية الدينية أو التأثير على الرأي العام من اجل دفعه لموقف معين سواء من خلال المنتديات الحوارية وبرامج الدردشة كأن يقف جهاز استخبارات لدولة ما خلف موقع يبدو انه معاد، ولكنها تستغله لجذب المتعاطفين معه وجمع معلومات عنهم وفهم أفكارهم، والدعاية والترويج لسياسية الدولة عن طريق مواقع الإنترنت التي تتبناها أجهزة الاستخبارات بشكل مباشر أو وقوفها بشكل خفي خلف مواقع أخرى وغالبا ما تكون مواقع خدمية كتلك التي تقدم خدمات بريدية أو

---

(1) انجيليو كودفيلا، المخابرات وفن الحكم " مترجم، محمد صبري الصاوي، الهيئة المصرية العامة للكتاب، القاهرة، الطبعة الأولى، ٢٠٠٦.

(2) توماس كويلاند (محرر) " ثورة المعلومات والأمن القومي " ، سلسلة دراسات عالمية ، مركز الإمارات للدراسات والبحوث الإستراتيجية ، العدد ٤٦، ٢٠٠٣.

(3) وجاء اتهام مهندس مصري بالتخابر لصالح الموساد الإسرائيلي في عام ٢٠٠٧ عن طريق التعاون لاختراق أنظمة الحاسب الآلي للهيئة النووية التابعة لوزارة الكهرباء والطاقة من خلال دس برنامج حاسب اولى على أجهزة الحاسب الخاصة بتلك الهيئة يتيح الاطلاع على المعلومات الخاصة بنشاط الهيئة ، والقيام بإنشاء موقع باسم حركي على البريد الالكتروني والتراسل من خلاله باستخدام شفره سرية . وجاءت تلك الحيثيات لتعبر وبوضوح عن وجود فعلي وملموس لمخاطر حرب المعلومات واستخدام شبكة الإنترنت في التجسس من قبل أجهزة الاستخبارات لدى العديد من دول العالم .وليعيد ذلك إلى الأذهان ما كشفت عنه صحيفة معاريف الإسرائيلية في ١٢-٤-٢٠٠٦ عن نجاح مهندس ومبرمج مصري يدعى "خالد شريف " بنقل أسرار منظومة حيتس الصاروخية الدفاعية إلى المخابرات المصرية وذلك عندما أدى عطل في برنامج التشغيل لتبادل عدد من المناقشات والرسائل المتبادلة حول تحديد وإصلاح عدد من العيوب التي ظهرت في برنامج كمبيوتر معروف باسم " MOTIF" مع المهندس في شركته العالمية بالقاهرة وهو البرنامج الرئيسي الذي تعمل من خلال منظومة الصواريخ وثارت مخاوف اسرائيلية من تمكن المهندس المصري من زرع برامج تجسس خاصة وان ٨٠ %من أداء الجيش الإسرائيلي يعتمد على أنظمة قتالية متطورة مرتبطة بالتشغيل الالكتروني .

دردشة عبر الإنترنت أو خدمة تنزيل البرامج المجانية. وهذا ما يساعد في جمع المعلومات والتنقيب عنها الخاصة بالدول أو الجماعات المعارضة لها سواء في الداخل أو الخارج للمساعدة في خلق رؤية واتجاه عام لديها بخصوصها والتعامل معها، و الاستفادة من كون الإنترنت عابر للحدود في خلق شبكة عملاء دوليين خارج حدود الدولة والمساهمة في إمدادها بشبكة معلومات عن الدولة التي يقيم بها، و التجنيد عن طريق مباشر بالإعلان عن حاجتها إلى من يتقنون لغة معينة أو أخرى، ويتم استخدام عنصري المال أو الجنس أو الهجرة حيث تكون شخصية العميل اما شخصية معادية للنظام القائم أو شخصية عادية تستطيع أن تقدم معلومات جيدة، ويتم ذلك عبر إحدى الوسائل مثل غرف الدردشة ويتحدثون عن أشياء قد تبدو تافهة ولكنها في ذات الوقت تشكل أهم المحاور التي تركز عليها أجهزة استقطاب المعلومات، مع احتفاظ العميل بخصوصيته ليكون أحساسة الرمزي بالحرية أكثر انطلاقا.

ويتم استخدام الفضاء الالكتروني في مسالة تعميم المعلومات وتبادلها بين أجهزة المخابرات داخل الدولة ذاتها أو بينها وبين دول أخرى حليفة لها لخلق تعاون ومبادرات مشتركة لمواجهه تهديد مشترك، و استخدام الإنترنت في التحويلات المالية للعملاء واستخدام غسيل الأموال كغطاء لعمليات التخابر ودفع الأموال، و الاستفادة من التداخل بين الفضاء الإلكتروني والفضاء الخارجي في عمليات التجسس على المنشآت المدنية الحيوية والعسكرية، وخاصة مع دخول تكنولوجيا الاتصال والمعلومات للمنظومة العسكرية لتحدث ثورة أخرى في الشئون العسكرية، وقد يشمل التجسس بث برامج على الجهاز في حال اتصاله بشبكة الإنترنت يتم من خلال كشف سرقه المعلومات التي بداخله أو عن طريق بث برامج خفية في ما بعد مرحلة تصنيع جهاز الكمبيوتر ويتم تصديرها إلي منشآت حيوية في بلد ما وذلك لسرقة معلومات عسكرية أو اقتصادية [1]

ثالثا:- حرب بلا إراقة دماء

اكتسب عمل أجهزة الاستخبارات حول العالم أبعادا هامة بفعل ثورة الاتصالات وتكنولوجيا المعلومات، وظهر الارهاب الالكتروني وحرب المعلومات فهي حرب بلا إراقة دماء وتقتصر أدواتها على جهاز كمبيوتر ونقطة اتصال بالإنترنت حيث تواجه أجهزة الكمبيوتر أخطاراً تصيب المخرجات في احد العوامل الثلاثة لها وهي القدرة على الوصول والسرية والسلامة والقدرة على الوصول تتمثل في قدرة الأطراف المخولة على أن تحصل على المعلومات تلك القدرة قد يجري الحد منها، أو أن يتم إزالتها إما عن طريق تدمير المعلومات أو البرامج أو الأدوات المادية أو عن طريق التدخل في نظام الكمبيوتر بشكل يصبح معها النظام مشلولا وعديم الفائدة أو عن طريق التدخل في ذاكره النظام أو في معالجه المعلومات أو سرقه معلومات دقيقة أو بث شائعات وبشكل يتم من خلاله أصابه عمليات التخزين والإدخال والمعالجة والإرسال والتحكم.

وتتميز حرب المعلومات وهجمات الارهاب الالكتروني بانها ليست مقيدة في المجال والمدى، وهدفها غير مأمون العواقب وقد يستغرق عده دقائق، وتعدد أطرافها، وهناك صعوبة في اكتشاف الهجوم

(1) Cullather Nick, Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyber war. Intelligence & National Security No.18,Winter 2003,pp:141-154

والذي يظهر متأخرا بعد تفاقم المشكلة وخاصة مع صعوبة تحديد هوية المهاجم، وتتقسم حرب المعلومات إلى نمطين هجومي ودفاعي تقوم بالهجومي في الغالب الدولة وأجهزة استخباراتها لما تمتلكه من إمكانيات ضخمة تؤهلها للقيام بذلك من اجل تحقيق أهداف سياسية وعسكرية أو لمجرد الإثارة وإظهار القدرات، و أما الحرب الدفاعية فهي تعمل على الحد من أعمال التخريب التي يتعرض لها وتختلف الوسائل الدفاعية باختلاف أدوات التخريب وطبيعة الأضرار التي تحدثها وذلك في حالة إذا ما تم استخدامها بجانب العمليات العسكرية التقليدية، أو حتى كسلاح مختار في الصراع بين عناصر ضد عناصر داخل الدولة كالقطاع الخاص أو ضد قوى خارجية، أو حتى استخدام الدول للمنظمات الإرهابية أو حتى أفراد أذكياء كبديل للحرب ضد الدول الأخرى وتصبح الأهداف السياسية هي الغاية والحرب والارهاب عبر الفضاء الالكتروني هي الأداة.(1)

رابعا:- صراع من اجل الحفاظ على القوة.

تستخدم الدول عبر أجهزتها الأمنية الإنترنت والفضاء الالكتروني بشكل عام في التجسس على مواطنيها وإحكام قبضتها على معارضيها، وفي مقابل ذلك فان الفرد قد يستخدم الانترنت وأجهزة تكنولوجيا الاتصال والمعلومات للتجسس علي الدولة لصالح الخارج أو عن طريق دعم دول أخرى، وخاصة مع وجود هيمنة اتصالية وتكنولوجية من الدول الكبرى التي تتجسس على الدول الصغرى، وتنتهج سياسات ثابتة من اجل دعم التجسس وأنظمته خاصة مع تنوع آلياته لديها عبر الإنترنت والاتصالات السلكية واللاسلكية والموجات والترددات ، ولأن العالم أصبح في حالة انكشاف معلوماتي تستطع الدول الكبرى توظيف ذلك لمصلحتها في الشأن الاقتصادي والسياسي والعسكري، وأدلى "رويرت ديفيد ستبل " عميل المخابرات الأمريكية السابق بتصريحات عن اتفاق سري وشراكة بين موقع جوجل على الإنترنت لإدارة معلومات العالم لصالح وكالة المخابرات الأمريكية وقد استخدمت الولايات المتحدة موقع جوجل لتحديد الشخصيات الإيرانية التي ستخضع لقائمة العقوبات الدولية، و طلبت بريطانيا من موقع جوجل للخرائط إزالة موقع القواعد العسكرية على برنامجها خشية تعرضها لهجمات.(2)

وأنشأت الولايات المتحدة موسوعة على الإنترنت اسمها "انتيليبيديا " في ابريل ٢٠٠٦ على غرار موسوعة ويكيبيديا البريطانية بما يساعد على إحداث تغيير جذري في ثقافة أجهزة الاستخبارات الأمريكية عن طريق المساهمه في تعميم المعلومات بين أجهزتها وذلك بعد أن انتهت بالعجز بعد ١١ سبتمبر ٢٠٠١ في الربط بين مختلف المعطيات التي بحوزتها وتكون بمثابة موسوعة خاصة يستخدمها فقط الموظفين لتخطي العوائق أمام انتقال المعلومات بين الأنظمة المعلوماتية غير المتجانسة المعتمدة لدى وكالات الاستخبارات الأمريكية.(3)

---

(1) عادل عبد الصادق، " الانترنت.. ساحة جديدة للتجسس الدولي " دراسات سياسية، جريدة الاهرام، ٥ مايو ٢٠٠٧

(2) جريده الاخبار المصرية ٢١ يناير ٢٠٠٧.

(3) جريدة الحياة اللندنية ، نوفمبر ٢٠٠٦

وظهـر اتجـاه للتحـول مـن أسـلوب الاسـتعداد لمواجهـة المخـاطر و معالجتهـا للتركيـز علـى اسـتخدام الأسلوب الاستباقي والوقـائي لمواجهتهـا، قبل أن يتمكـن العـدو مـن معرفـة نقـاط الضعف داخل النظـام المعلوماتي الأمريكـي أو تدميره، وأصبح للاستخبارات دور فاعل وليس فقـط مراقب فقامت بإنشاء موقـع سـري شبيه بموقـع"My Space" وموقـع "Face book" ، حيـث يتبـادل مستخدمو الموقـع المعلومـات والأخبـار فيما بينهم، و كـذلك هو الحال مع أفراد الاستخبارات الـذين سيكونون قـادرين علـى مقارنـة الملاحظـات حـول صـور الأقمـار الـصناعية الملتقطـة للمواقـع النوويـة في كوريـا الـشمالية، أو المتمـردين العـراقيين أو الصواريخ الصينية أو إيران، وفي ٢٢ سبتمبر ٢٠٠٨ تم إطلاق موقع أمريكـي يسمى بـ"A-Space "[1].

ويـتم إرسـال التقـارير عـن طريـق كـل وكالـة اسـتخباراتية كمـا يـتضمن الحمايـة ضـد المتسللين، للمـساعدة في ربـط ١٠٠ ألـف شـخص عمـلاء للأجهـزة الاسـتخباراتية، بالإضـافة إلى المـدونات كوسـيلة لجمـع المعلومـات والاطـلاع المشترك عليهـا [2]. وهنـاك برنامجاً لتتبـع مـصدر المـواد الـتي يحررهـا مستخدمو ويكيبيـديا ويعـرف باسـم "ويكيسكانر"حيـث تم الكـشف مـن خلالـه عـن دور وكالـة الاسـتخبارات الأمريكية في تحرير المواد وإزالة بعضها على موقـع الموسـوعة الحـرة على الإنترنت، ويقـوم هـذا البرنـامج علـى مـسح حـوالي خمـسة ملايـين وثلاثمائـة ألـف عمليـة تنقـيح أو إضـافة ويتقـصى مـصدرها ليـصل إلى عنوانهـا الالكترونـي علـى الإنترنـت[3]، وأطلقـت الإدارة الأمريكيـة حملـة سـرية تقـضي بـزرع مواقـع علـى الإنترنت وعناوين بريد الكتروني وهمية لإرباك المنظمات "الإرهابية " وزرع الشقاق والشك في صفوفها[4].

وهنـاك الرقابـة المركزيـة للولايـات المتحـدة علـى الإنترنـت وكـذلك توجيـه أقمـار تجـسس لرصـد اتصالات الأجهـزة السلكية واللاسلكية عـن طريـق التقـاط الإشـارات الكهرومغناطيسية وإرسـالها مـن جميـع انحـاء العـالم لتتحـول إلى الولايـات المتحـدة حيـث تـدخل إلى أجهـزة كمبيـوتر متطـورة لتحليلـها ويـشارك في عمليـة الالتقـاط مـشروع أيـشلون، وهـو نظـام عـالمي مخـصص لاعـتراض معظـم الإشـارات الرقمية في أنحاء الكـرة الأرضية وتديره المخـابرات الأمريكيـة بالتعاون مـع أجهـزة مخـابرات في أربـع دول أخري هـي بريطانيا ونيوزيلندا واستراليا وكنـدا، بدايـة مـن اتصالات الأقمـار الصناعية ونهايـة بالحركـة المختلفـة علـى شـبكة الإنترنـت بمـا في ذلـك رسـائل البريـد الالكترونـي والملفـات الـتي يـتم تبادلهـا عـبر الـشبكة، بالإضـافة إلـي مجموعـة أقمـار صـناعية مخصـصة لنقـل فيضان البيانـات اليـومي إلـي مراكـز التحليل والفحص الأرضية، بالتعاون مع شبكة الأقمار التجسسية حول العالم.

وهنـاك تحالفـا اسـتخباراتيا يتكـون أعـضاؤه مـن الـدول المتحدثـة بالانجليزيـة يـسمي "يوكـوزا" (UKUSA)،حيـث وضـعت هـذه الـدول محطـات تجـسس الكترونيـة وأقمـارا صـناعية لالتقـاط حركـة الاتـصالات اللاسـلكية وإشـارات الأقمـار الـصناعية والموجـات اللاسـلكية الـصغرى واتـصالات الهواتـف النقالة ، ولدى كل عضو من تحالف"يوكوزا" مهام محددة لمراقبة أجزاء مختلفة من العالم، وفي ابريل

---

(1) جريده الشرق الأوسط، ٣٠ سبتمبر ٢٠٠٧
(2) جريدة الشرق الأوسط ٣-٩-٢٠٠٧
(3) جريدة الشرق الأوسط ١٩-٨-٢٠٠٧
(4) جريدة الحياة اللندنية ، ١٩ مارس ٢٠٠٨

٢٠٠٤ قرر الاتحاد الأوربي إنفاق ١١ مليون يورو من أجل تطوير نظم اتصالات مؤمنة وفق مشروع أطلق علية اسم SECOQC [1] وهو نظام يعتقد أنة لا يمكن اختراقه من أي برامج تنصت أو تجسس في العالم.

وفي فبراير ٢٠٠٥ قامت أجهزه الاستخبارات الأمريكية بإجراء "مناورة الكترونية " سميت بعاصفة الحواسب'Cyber Storm' على غرار عاصفة الصحراء، حيث وضعت البني التحتية الحيوية الامريكيه التي تشمل شبكات الكهرباء والنظم المصرفية تحت محاكاة التعرض لهجوم، وتقوم الصين وروسيا بفحص شامل للأجهزة الالكترونية المستوردة من الولايات المتحدة أو من حلفائها قبل دخولها أراضيها وذلك منعا لمحاولات التجسس أو إرسال رسائل مشفرة إلى مصدر استخباراتي معادي.ووقع الرئيس بوش الابن في ٨ يناير ٢٠٠٨ على تعليمات تقضي بتوسيع دور الاستخبارات في مراقبة الإنترنت للحماية ضد تصاعد الهجمات على أنظمة الكومبيوتر في المؤسسات الفيدرالية وحملت اسم التوجيه الرئاسي للأمن القومي رقم ٥٤ و ٢٣.

وبموجب هذه المبادرة الجديدة سيقوم فريق عمل بتنسيق الجهود لتشخيص مصدر الهجمات ضد أنظمة الكومبيوتر الحكومية. وكجزء من تلك الجهود ستعمل وزارة الأمن الداخلي على حماية الأنظمة بينما يعد البنتاجون استراتيجيات لهجمات مضادة على المتطفلين.وذلك ردا على طائفة من الهجمات على شبكات وزارات الخارجية والتجارة والدفاع والأمن الداخلي. مع وجود اتهام لمواقع انترنت صينية متورطة في عدد من أكبر الهجمات منذ عام ٢٠٠٥، وبينها بعض الهجمات على مختبرات الطاقة النووية وشركات تعاقدات دفاعية. ولدى وكالة الأمن القومي خبرة خاصة في مراقبة طائفة واسعة معقدة من أنظمة الاتصالات الخارجية، وتهدف المبادرة للقيام بدور في رقابة الشبكات الداخلية ضمن برنامج المراقبة الداخلية الحكومي وخطط توسيع دور وكالة الأمن القومي في الأمن الإلكتروني. باسم" المبادرة الالكترونية" التي تهدف إلى تأمين شبكات الكومبيوتر الحكومية ضد هجمات من أعداء أجانب وغيرهم وتبلغ تكلفتها الأولية مليار دولار.[2]

وفي إسرائيل كان هناك اهتمام مبكر لأهمية الإنترنت في عالم التجسس حيث قامت بتأسيس مكتب المخابرات عبر الإنترنت عام ٢٠٠١ تحت قياده ضابط المخابرات الإسرائيلية "موشى اهارون "بالتعاون مع ضابط من وكالة الاستخبارات المركزية الأمريكية،وتم الكشف عن شبكة تجسس إسرائيلية في مايو ٢٠٠١ لاستقطاب شباب العالم الثالث وخاصة محور الصراع مع إسرائيل ومحور العداء لأمريكا في أمريكا اللاتينية . وظهرت تقارير استخبارتية تطالب بالتركيز على كل من الصين واندونيسيا وفرنسا ونيجيريا وفنزويلا ومصر، ولاشك أن هناك تعاوناً أمريكيا إسرائيليا عبر الأقمار الصناعية وعن طريق المواقع البريدية التي تقدم خدمة الدردشة ، وقد أطلق موقع المخابرات الإسرائيلية حملة لتجنيد اللبنانيين إبان حربها مع حزب الله وقدمت عدة إغراءات مادية، وكذلك طلبت وكالة المخابرات المركزية تجنيد ٢٠ ألف عميل حول العالم يتقنون اللغة العربية.

---

(1) جريدة الأهرام ٤ يناير ٢٠٠٦

(2) Ellen Nakashima," **Bush Order Expands Network Monitoring**", Washington post, .27-1-2008.

وقد تبنت إسرائيل ""إستراتيجية الطين" MUD Approach، وهي ثلاثة أحرف، تمثل ثلاثة أساليب هي (الرصد، الاستخدام، العرقلة)Monitoring Using and Disrupting.[1] ويقصد بـ(الرصد)، رصد الأفكار والدوافع وطريقة التفكير لدى زوار ومستخدمي هذه المواقع، من أجل تحديد الأهداف والخطط، أو أي هجوم محتمل يفكر به طرف ما (الإرهابيون). وتقوم عملية الرصد أيضا، بمتابعة الخلافات والمناقشات الداخلية التي تدور بين الجماعات والأفراد، لمعرفة اتجاهات التفكير ومعرفة المعتدلون و"المتطرفون".

و يقصد بـ (الاستخدام)، استخدام هذه المواقع والمشاركة فيها من أجل معرفة أماكن وهويات (الإرهابيين) وتحديد دولهم، والتعرف على مشرفي المواقع والمنتديات وغرف المحادثة، والتواصل مع شركات الاستضافة من أجل معرفة جميع هذه المعلومات. في حين يقصد بـ (العرقلة) أو الإضرار بهذه المواقع، إما تعطيل هذه المواقع بالوسائل السلبية أو الإيجابية (كما عبرت عنها وثيقة المؤتمر)، بمعنى التدمير الفعلي لهذه المواقع عن طريق الفيروسات أو إرسال (سيول) من المعلومات إلى الموقع لتعطيله. مثل قيام إسرائيل بالتجسس الكترونيا على عمل المصارف الإسلامية بهدف مراقبة الحوالات المالية الجارية في هذه البنوك في إطار الحرب الأمريكية على الإرهاب؛ وبدعوى أن هذه المصارف تشكل إحدى أدوات وأذرع تمويل العمليات الإرهابية، ويزعم تمكينها المالي للأصولية الإسلامية المتطرفة، ومدها بالأموال اللازمة عن طريق التبرعات وغيرها للتأثير أو العمل على إعاقة الجهاز المالي والمصرفي الإسلامي.

وفي عام ٢٠٠٢ فتح جهاز الاستخبارات الروسي (FSB) تحقيقا ضد عميل لمكتب التحقيقات الفدرالي الأميركي (FBI) يدعى مايكل شولر، بعد اتهامه بالتسلل إلى أنظمة المعلومات الأمنية الخاصة بالمخابرات الروسية. بالمساعدة من قرصانين روسيين هما "فاسيلي جورشوك "و"أليكسي إيفانوف "،وساعداه عن غير قصد في الدخول إلى نظام أجهزة الاستخبارات الروسية.[2] وهناك منظمة تُطلق على نفسها اسم "خبراء الإنترنت الأمريكان" تقوم بمهاجمة المواقع التي تعتبرها إرهابية، ونظراً لإدراك أهمية شبكة الإنترنت في ازدياد موجة التطرف الإسلامي، فإن استخبارات الدول الغربية تراقب الإنترنت جيدا، وتكثف من حملاتها المناهضة لمهاجمة الكثير من المواقع الإسلامية المتطرفة بانتظام وتلقى اجهزة الاستخبارات العون من مجموعات من الهاكر ومهاجمي مواقع الإنترنت تابعين لهذه المنظمة للهجوم على المواقع الجهادية.[3]

وقد قاد عملية اندماج الإنترنت بالاتصالات أجهزة الاستخبارات الأمريكية إلى اعتقال خالد شيخ محمد العقل المدبر لأحداث ١١ سبتمبر ٢٠٠١، كما قادت إلى مقتل "أبو الليث الليبي "حيث تم تحديد مكانه عن طريق قيامه بالاتصال بهاتفه المحمول عن طريق الأقمار الصناعية من جانب أجهزة الاستخبارات الأمريكية [4]، واستخدمت إسرائيل هذه الوسيلة لقتل واستهداف القيادات الفلسطينية، ومن الأمثلة الأخرى لاستخدام التقنيات في تنفيذ العمليات العسكريّة تلك التي تحدث في العراق

---

[1] عمر عبد العزيز مشوح،" إستراتيجية (الطين) الصهيونية لتطويق المواقع الإسلامية"، مرجع سابق ذكرة .

[2] موقع قناه الجزيرة الفضائية في ٢٠٠٢/٨/١٥.

[3] موقع اخبارنا اخر زيارة (١٣-٥-٢٠٠٧ )
(http://www.akhbaruna.com/node/454?PHPSESSID=0e5dc768888e742bcfd8d5083367fac6)

[4] جريدة الحياة اللندنية ٢ فبراير ٢٠٠٨ .

ويستخدم فيها المهاجمون برنامج "جوجل إيرث" الذي يعرض المواقع العسكريّة للمخيّمات العسكريّة البريطانيّة (مثل مواقع المباني والمخيّمات والآليات التي تحتوي على أسلحة خفيفة وأماكن تناول الجنود للطعام وحتى المراحيض الموجودة في المعسكرات، بالإضافة إلى إحداثيات الطول والعرض الدقيقة للمخيمات) وبيع هذه الصور في أسواق البصرة بشكل يوميّ وشنّ الهجمات عليها.

وقد طلبت قوات التحالف في العراق من "جوجل" حذف الصور الحديثة لهذه المواقع، بالإضافة إلى طلب إسرائيل أمرا شبيها يتعلق بمواقع سلاحها الجوي ومطاراتها العسكرية، (1)"بعد نشر جنود لصور تكشف أسرارا من الثكنات الإسرائيلية ومقرا لقيادة الجيش وأجهزة اتصال حساسة داخل المقر وقواعد عسكرية وأبراج التحكم ، وأنظمة التسلح المختلفة من زوارق حربية وأنواعا وكميات من الأسلحة التي تستخدمها وحدات المشاة أضافه إلى أسماء وأعداد وحدات مشاه واستطلاع وساحات تدريب وتشكيلات قتالية وتدريبات سرية ، وكان ذلك مصدر قلق لوزارة الدفاع الإسرائيلية وخشيتها من ان استغلال أجهزة استخبارات أجنبية أو مجموعات "إرهابية " ".(2)

وعمد مكتب المباحث الفيدرالي الأميركي لبناء أكبر قاعدة معلومات تتضمن الأوصاف الجسدية، وهو مشروع سيمنح السلطات الأميركية قدرات غير مسبوقة في التعرف على الأفراد داخل الولايات المتحدة. وتتضمن قاعدة البيانات تفاصيل رقمية للوجه والبصمات وأنواع راحة اليد وبيانات تفاصيل الوجه، والعلامات البارزة، بغرض كشف الجرائم والتعرف على المجرمين والإرهابيين.(3)

## المطلب الثاني:

## استخدام الجماعات الإرهابية للفضاء الالكتروني

اولا : الجماعات الارهابية الرسالة والمضمون والدوافع

استغلت الجماعات على كافة أشكالها وأنماطها الفكرية المختلفة وغيرها تلك المزايا كعنصر حيوي لدعم وتحقيق أهدافها ومنفذ لوجستي داعم وحاضن للنشاط الإعلامي لها في مناطق مختلفة من العالم، ليشكل مجتمعا افتراضيا يتحول من مجموعة قليلة من الناس متوزعة جغرافيا لتشكل مجتمعا خاصا بها يساعدها علي الالتحام والتواصل الدائم، الأمر الذي يوهم البعض بأن هذا المجتمع غير محدد الأبعاد الكمية، وهو ما كان له دور كبير في تضخيم الصورة الذهنية لقوة وحجم تلك المجموعات.

و يعتبر الإرهاب سلاح الضعيف الذي لا يقدر على شن حرب ضد الدولة، فعن طريق الإرهاب يمكن إلحاق الأذى ومحاوله هزيمة القوة العظمى، وهذا ما يتضح في الجماعات الثانية والميليشيات العنصرية والأصوليات الدينية وبعض الأقليات التي لا تملك القوه، ويكون الإرهاب وسيلة لتأكيد الهوية وجذب

---

(1) Martin Asser," **Israel army in Face book clampdown** ",BBC News, 11 April 2008. (http://news.bbc.co.uk/1/hi/world/middle_east/7343238.stm)

(2) **Facebook at center of Israel security scandal.** Israel today. April 14, 2008. ( http://www.israeltoday.co.il/default.aspx?tabid=178&nid=15720)

(3) جريده الشرق الأوسط، ٢٣ديسمبر ٢٠٠٧.

الانتباه والاهتمام وقد يكون وسيلة من وسائل الصراع أو يكون من وجهه نظر من يقومون به نهاية الصراع حيث تدمير هوية العدو. ويتعلق بالسماوات المفتوحة والفضاءات التكنولوجية، وكذلك يكون وسيلة لتحقيق أهداف مستقبلية عبر تحطيم الحاضر للوصول إليها، حيث التحطيم يكون بداية لظهور شيء معين من بين ركامه، ويكون مدفوعاً بقيم أخلاقية أو ثقافية.[1]

ويكون منشأ الإرهاب اما بدافع الثأر وتوقيع العقوبة عن أخطاء الماضي، اوالقدرة على الإلهام وإعادة الإحياء والتبشير بعهد جديد، ففي الأول يكون العنف استراتيجياً بشكل كبير والأهداف محددة وواضحة، بينما الثالث يعبر عن كيفية تغيير العالم عن طريق الإرهاب. وبالرغم من تلك الاختلافات إلا أنها لا تعني بالضرورة وجود تمايزات ففي كل الأحوال هناك عنف، وتأتي هذه الأسباب لتستمر في عصر الثورة المعلوماتية. فالإرهاب بطبيعته ليس ظاهرة ثابتة في دائمة التغير حيث يغير مرتكبوه ملامحهم ووسائلهم ليتكيفوا مع زمانهم ومواقفهم ولضمان تحقيق ما يهدفون إلية .

وقد استفاد الإرهابيون أيضا من ذلك التطور السريع في تكنولوجيا الاتصال حيث يستطيعون ببساطة شراء المنتجات التكنولوجية التجارية والاستفادة مما تم انفاقة في البحث والتطوير، وليتمكنوا من الحصول على أجهزة كونية المدى فائقة السرعة متنوعة ومعقدة ومشفرة وبدون أية تكاليف باهظة، وأتاحت شبكة الإنترنت الفرصة للحصول على أسهل الوسائل لاكتساب المعلومات وإصدار الأوامر والسيطرة على عملياتهم المخططة [2].

و ظهر التزاوج بين الإنترنت والإرهاب بشكل أكثر وضوحا بعد إحداث الحادي عشر من سبتمبر ٢٠٠١، وما تلا ذلك من الحملة الأمريكية علي'الإرهاب' وحدوث مواجهة بين تنظيم القاعدة وحلفائها من جانب والولايات المتحدة ومؤيديها من جانب أخر ولم تقتصر تلك المواجهة علي المجال المادي الواقعي بل انتقلت إلي الفضاء الإلكتروني وأصبح هناك حملة إعلامية مواكبة للحملات العسكرية من جانب الطرفين تم فيها استخدام الإنترنت وفي العام ١٩٩٨، كان لدى أقل من نصف المنظمات المصنفة من قبل وزارة الخارجية الأميركية كمنظمات إرهابية مواقع إلكترونية. وبحلول نهاية العام ١٩٩٩ كانت جميع هذه الجماعات الإرهابية تقريبا قد أوجدت لنفسها حضورا على الإنترنت. وأصبح لجميع الجماعات الإرهابية النشيطة حضور واحد على الأقل على الإنترنت، وفي الفترة الممتدة من العام ١٩٩٨ إلى العام ٢٠٠٧ إلى جود أكثر من ٥ آلاف من المواقع والمنابر وغرف المحادثة الإلكترونية التابعة.

والتي تأتي في صورة استخدام الإرهاب الإلكتروني في التأثير على الرأي العام حيث تدور معركة ذات طابع فكري وثقافي، أو كأداة لإحداث خسائر اقتصادية بالتلاعب في مرافئ الاقتصاد العالمي وتحقيق ضعف الأنظمة السياسية، أو استخدامه بالتوازي مع القيام بعمل إرهابي مادي سواء في التنسيق له أو جمع معلومات عنه، تساعد في توفير درجة عالية من للتنظيم و دعم عملية صنع القرار عير

---

[1] حسن الشامي، "وسائل الاتصال وتكنولوجيا العصر "، الهيئة المصرية العامة للكتاب، القاهرة، ١٩٩٧، ص ص ٣٠-١٩٠.
[2] تقرير اللجنة القومية الأمريكية عن الهجمات على الولايات المتحدة " " تحرير وتقديم "د. حسن أبو طالب"، الفصل الثالث، مركز الدراسات السياسية والإستراتيجية بالأهرام، القاهرة، مايو ٢٠٠٦، ص ١٣٢ .

الشبكات، وما توفره من سرعة تدفق المعلومات ورخصها وكونها أكثر أمانا ومتعددة الجوانب، وإمكانية استخدام التكنولوجيا كسلاح هجومي ودفاعي.

أما عن المضمون فان الجماعات المتطرفة تمتلك بجميع أشكالها ومختلف توجهاتها السياسية من امتلاك مواقع علي شبكة الإنترنت، ومنها من يمتلك أكثر من موقع، يقدم خدماته بأكثر من لغة، وتهدف إلي التعريف بالتنظيم وتاريخه، ومؤسسيه وأبطاله، وأنشطته، وخلفياته السياسية والاجتماعية، وأهدافه السياسية والأيديولوجية، وأحدث الأخبار، والنقد الشديد للأعداء كما تهدف رسالة المواقع بصور متعددة؛ منها الدعم الفكري لهذه التنظيمات وتبجيل أفرادها، أو مهاجمة المعتدلين والمفكرين أو مهاجمة الحكومات والأجهزة الأمنية، وقد تسعي تلك المواقع للتغطية علي موقفها الداعم للإرهاب بالسماح بنقد يسير، والاستناد في ترويج فكرها الى بعض الكتابات الإيديولوجية والدينية، وإلحاقها بتفاسير معينة وقصص تاريخية وضعت ضمن تأويل متعسف لكي تقنع المتلقي بمشروعية عملها حيث يتم استغلال الدين باعتباره مظلة إيديولوجية تؤهلها لاستقطاب عناصر جديدة، كما يتم نشر تلك الأفكار وإدارتها من قبل أشخاص ذوي أفكار أحادية لا تسمح بوجود احد ينافسها أو يعرض رأيا يخالفها.[1]

- <u>تهدف الرسالة الخاصة بتلك المواقع ثلاثة أنماط من الجمهور</u>: النمط الأول هو جمهور المؤيدين الحاليين والمحتملين وذلك عبر تقديم الموقع لهم معلومات مفصلة حول أنشطة المنظمة وسياساتها الداخلية وحلفائها ومنافسيها، وعادة ما يكون هذا الجمهور هو جمهور محلي، والنمط الثاني من الجمهور هو الرأي العام العالمي وهو الجمهور غير المتورط مباشرة في الصراع، ولكن لديه بعض المصالح في القضايا المطروحة.[2] و يضم هذا الجمهور المستهدف الصحفيين ووسائل الإعلام التي تستخدم مواقع هذه التنظيمات للحصول علي وجهات نظرها، ويساعدهم في ذلك طرح خدمات المواقع بلغات عدة.، وأخيرا يتمثل النمط الثالث في الأعداء وتسعي مواقع هذه التنظيمات من استهدافهم إلي إضعاف معنوياتهم من خلال توجيه التهديدات وتعزيز الشعور بالذنب لديهم إزاء التصرفات والدوافع .[3]

- <u>تستخدم التنظيمات المتطرفة علي اختلافها ثلاثة خطابات في الدعاية:</u>

الخطاب الأول: هو الادعاء بأنه ليس أمامها خيار سوي التحول إلي العنف والذي يقدم كضرورة أجبر عليها الضعيف باعتباره الوسيلة الوحيدة التي يرد بها علي العدو الظالم، ويتم التأكيد علي أعمال القوة التي تستخدمها الحكومات والأنظمة ضدها وضد تنفيذ مطالبها، كما يتم استخدام مصطلحات كالذبح والقتل والإبادة، وتصف المنظمة نفسها كمضطهد تطاردها القوي الكبرى أو الدولة القوية، وهذا ما يحول التنظيم وأتباعه إلي ضحية.الخطاب الثاني: والمرتبط بشرعية استخدام العنف، هو هيمنة وعدم شرعية العدو، فأعضاء الحركة أو المنظمة يعتبرون أنفسهم مقاتلين من أجل

---

(1) عادل عبد الصادق ،" المتطرفون وحرية التعبير على الانترنت بين الامن والانفتاح"، مرجع سابق ذكرة .
(2) حسن عماد مكاوي، "ليلى حسين السيد، " الاتصال ونظرياته المعاصرة " "، الدار المصرية اللبنانية، القاهرة، ١٩٩٨، ص ص ٢٣-٣٤.

(3) Gabriel Weidman, <u>How Modern Terrorism Uses the Internet</u>, The United States Institute of Peace, www.terror.net, Special Report No. 116, March 2004.

الحرية، ومجبرين بما يتنافى وإرادتهم علي استخدام العنف، نظرا لأن العدو يسحق كرامة وحقوق شعبهم أو جماعتهم، وأن عدو الحركة أو الجماعة هو الإرهابي الحقيقي.أما الخطاب الثالث هو الاستخدام الواسع لمبدأ اللاعنف في محاولة لدرأ الصورة العنيفة عنها، فعلي الرغم من كون تلك الجماعات هي جماعات عنيفة، إلا أن الموقع المرتبطة بها تدعي سعيها للحلول السلمية، وان هدفها النهائي هو التسوية الدبلوماسية التي تتحقق عبر المفاوضات والضغط الدولي علي النظم الجائرة.[1]،وبرزت العلاقة ما بين الفضاء الالكتروني والارهاب من خلال عدد من المظاهر لعل اهمها :

ثانيا : تصاعد دور الدين في العلاقات الدولية وظهور الأصوليات الدينية

يشهد الفضاء الالكتروني عمليات الدمج مع الثقافات المختلفة وتحولها لصور رمزية سريعة الانتشار والتحرك والتفاعل مع الآخرين، وإنتاج وإدارة وتوزيع العملية الثقافية في العالم وظهرالدين كأحد مكونات تلك العملية لتدفع الأفراد للتعرف على أوجه عديدة للإنسانية ومتمايزة عن نظرتهم الأحادية، وبشكل يتم فيه التفاعل إلى حد الصدام ما بين التقليدية والقيم المحلية وما يفرضه الفضاء الالكتروني من تحد لتلك القيم والجماعات التي تدافع عنها في صورتها التقليدية.

ويأتي هذا مع تراجع الإعلام الجماهيري لصالح الالكتروني حيث لا سيادة للدولة علية وقدرته على الانتشار وقدرته الفائقة على تضخيم جزئيات إعلاميا بعيدا عن أهميتها النسبية عبر مواقع الإنترنت، والتي انصب جزء منها على بث الكراهية الدينية مع المختلف الديني وأصبح الإنترنت ظاهرة مركزية في عالم الحداثة وما بعدها التي تتفاعل مع التقاليد الدينية للجماعات الأصولية، في ظل مخاطر صراع حضاري يتم تغليفه بطابع ديني مما يضفي على الصراع عمقه وطول أمدة وتوالي خسائره.

وقد وصل عدد مواقع الإنترنت في العالم نحو ١٠٠ مليون موقع في عام ٢٠٠٧ وبلغ عدد مستخدمي الشبكة نحو٣ مليار مستخدم حول العالم ، ويستخدم عدد من المنظمات الإرهابية حول العالم، والتي من ضمنها حركة ايتا بإقليم إلباسك باسبانيا ومنظمتي "توباك امارو" و"الطريق المستنير" في بيرو، ومنظمة" لاشكار اتويبا "في أفغانستان بالإضافة إلى المتمردين في العراق والشيشان وغيرهم الكثير[2]، وذلك للاستفادة من جمهور واسع للرسالة الإعلامية، و الاتصال الدائم عن طريق تكنولوجيا الاتصال لإعادة تشكيل الحدود بين المجالين العام والخاص، وارتباط البشر بها ليس فقط في استخدامها اليومي ولكن كذلك في نقل القيم والرموز المرتبطة بها .

وقسم الإعلام الالكتروني الجمهور لفئات ومجموعات صغيرة و بدأ هذا التنوع يزيد بدوره من التشتت الثقافي والتمحور حول موضوعات محددة، وفقدان التماثل الثقافي الذي ميز المجتمعات القومية وتحول الإعلام الجماهيري الى اعلام فئوي يستخدم لإذكاء الصراعات العنصرية وتنمية اتجاهات الكره لدى الكثير من الفئات المناهضة لفئات أخرى، و أصبحت هذه السمات تتمتع بحضور دائم لمنظومة الإعلام الالكتروني ووسائله في نطاق تطور تقنيات المعلومات المعاصرة، وزحزحة قوة

---

(1) Gabriel Weimann ," Terror on the Internet: The New Arena, The New Challenges", Washington, United States Institute of Peace Press, 2006. p309.

(2) Gabriel Weimann" **Terror on the Internet**" ,Potomac books , ,Inc, April 2006 pp 20-323.

الدولة القومية وركائزها لصالح فئات وجماعات كفاعلين من غير الدول، وأخذت التكنولوجيا مكانها ضمن سياقات مجتمعية تملك خصوصيات تاريخية لكنها تندرج في الوقت نفسه ضمن الحراك الاجتماعي العالمي.

و يتميز الإعلام الالكتروني برخص الأداة، وضعف الرقابة وتنوع وسائلة وانتشاره وتخطية للحدود وقدرة أي فرد على التأثير فيه، وشكل نوعا اجتماعيا جديدا من التواصل وهو كثيف دون شك لكنة صادر ومتلقي ومحسوس من قبل كل فرد على حده، و تم تملكه في إنحاء العالم كافة من قبل كل الحركات الاجتماعية للتأثير على وسائل الإعلام الكبرى والتحكم في المعلومات وتكذيبها إذا لزم الأمر أو حتى إنتاجها وقد تم تملكه في أنحاء العالم كافة من قبل كل الحركات الاجتماعية، لكنها ليست أبدا الوحيدة التي تستخدم آلية التحريك والتنظيم الجديدة وأصبحت الحركات الاجتماعية وكذلك الأفراد قادرين على التأثير على وسائل الإعلام الكبرى والتحكم في المعلومات وتكذيبها إذا لزم الأمر أو حتى إنتاجها.[1]

ويختلف كل من تكنولوجيا المعلومات والدين في الاستجابة السريعة للتغير بينما يتفقان في الرغبة في الانتشار عبر الكون، فالدين بطبيعته يستند إلى مجموعه من القواعد والمعايير الأخلاقية التي لا تقبل التطور أو الذود عنها لأنها تكون من أسس ذلك الدين، أما التكنولوجيا فإنها بطبيعتها متغيرة غير ثابتة بتغير الابتكارات والمهارات الفردية، إذا فإننا أمام جانب يميل للمحافظة بطبيعته وجانب يميل إلى التغير باستمرار حيث لا ترتبط إلا بمعايير السوق والمال والابتكار.[2] وقد استفادت الأديان كغيرها من الأفكار من الفضاء الالكتروني لتوفير ماده مستمرة وسريعة ومتفاعلة عن الدين وعن الرد على منتقديه والتأكيد على النزعة الكونية له، و كان الإسلام والمسيحية لهم السبق لاعتمادهما على الدعوة التبشيرية بخلاف اليهودية وبث مبادئهما والوعي بها وتجنيد أتباعهما، وليصبح الإنترنت مجموعه مختلفة من الثقافات تعبر عن نفسها في سياقات ثقافية مختلفة.

وبالرغم من الاعتقاد السائد بان الأصوليين هم أكثر الناس معاداة للحداثة والتكنولوجيا إلا أن الرؤية التحليلية لهم توضح أنهم لا يعارضون الحداثة بقدر انتهاكها لقيمهم المحلية والتقليدية، حيث سعوا بمختلف أشكالهم الفكرية والسياسية والدينية لاستخدام الإنترنت لخلق نمط جديد ومختلف يتناسب مع مجتمعاتهم ويواكب السياق الاجتماعي المشترك وتغير طبيعة التفاعل مع المؤسسات الاجتماعية. مع تأثر النظام الاجتماعي وتغير طبيعة التفاعل مع المؤسسات الاجتماعية مع الاتصالات التقنية.[3]

وتؤمن الحركات الأصولية الدينية بوجود صارم للقيم وتتمتع بدرجة عالية من التماسك الداخلي بين أعضائها بمعزل عن العالم الخارجي الذي يحيط بها ، فهي تريد العودة للتاريخ حيث المصدر النقي

---

(1) مانويل كاستلز "وسائل الاتصال الجماهيرية الفردية الجديدة" مجلة لوموند ديلوماتيك ، أغسطس ٢٠٠٦.

(2) عادل عبد الصادق ،"حقيقة دور الإنترنت في بث الكراهية الدينية في العالم ، ملف الأهرام الاستراتيجي ، مركز الدراسات السياسية والاستراتيجية بالأهرام ،عدد ١٤٤، ديسمبر ٢٠٠٦.

(3) S. Rafaeli., and, F. Sudweeks "**Interactivity on the nets in network and net play :virtual groups on the internet** , (eds) F.sudweeks and M.maclaughlim, Menlo park CA:mit press 1998 ,pp 173-189.

للمعتقدات بدون أي تغيرات براجماتي ، و تأخذ تلك الأصوليات اتجاها فكريا فقط أو اتجاهاً عسكريا عن طريق ما تراه محاولة لهدم الواقع للعودة للمستقبل الذي منبعه التاريخ حيث القيم الأصيلة ، وتشترك في ذلك كل الجماعات الأصولية سواء التي تتبع الديانات السماوية أو الوضعية على حد سواء،و سعى الأصوليون على مختلف أشكالهم الفكرية والسياسية والدينية لاستخدام الفضاء الالكتروني لخلق نمط جديد ومختلف يتناسب مع مجتمعاتهم ويواكب السياق الاجتماعي المشترك.[1]

واستخدمت الأصوليات على مستوى العالم الإنترنت من خلال أربعة أبعاد وهي الهراركية، والسلطة الأبوية، والتنظيم، والعزلة، وأصبح أداة وجزءاً من نشر الثقافة الأصولية، وأداة لتغيير الطرق التقليدية للحياة وساهمت في وجود قوانين غير مكتوبة تتحكم في سير تلك الأصولية الدينية، باستخدامها الإنترنت كأداة للدفاع للحيلولة دون استخدمها كأداة للهجوم عليهم وعلى معتقداتهم الثابتة، وليصبح العالم أمام تكنولوجية الثقافة للترويج للقيم الثقافية المحلية، والتي أصبحت معرضة للانتهاك تحت سقف العولمة الثقافية حيث درجة التنميط لقيم واحدة تعبر عن هيمنة ثقافة معينة.

وتنقسم المجتمعات المعاصرة في تأثرها ضمن ثلاثة أنماط متداخلة ومتفاعلة: وهي <u>التراتبية الاجتماعية</u>: حيث أن العلاقات بين الفئات الاجتماعية غالبا ما تحكمها علاقات تميل إلى الهيمنة ضمن هذا السياق و الدور الذي تقوم به التكنولوجيا الرقمية في إنتاج وأعاده إنتاج هذه التراتبية وتؤثر التكنولوجيا على <u>الوعي الجماعي</u>: ولا يمكن حصر الحياة الاجتماعية في علاقات الهيمنة ذلك إن الأفراد عاده ما ينتمون إلى جماعات داخل الجماعة الاجتماعية الكبرى التي نطلق عليها المجتمع، كما إن هناك تأثيراً للتكنولوجيا على <u>الهوية الشخصية</u>: حيث تتشكل غالبية المجتمعات المعاصرة من أفراد يغلب عليهم تمركزهم حول ذواتهم مع ما يستتبع ذلك من أثار تمس طبيعة العلاقة بذواتهم وبالآخرين فكل فرد هو تعبير عن خصوصية ذاتية.

وتكمن أهم مسببات زرع الكراهية حين يصبح الفضاء الالكتروني واستخدام موقاع الانترنت المعبرة عن كافة الاديان والثقافات والتي يمكن ان يساهم في انتاجها اناس يحملون رؤى متطرفة او انها على غير وعي او سطحية المعرفة مع حرية استخدام تلك المواقع ، حيث يتم ابراز كل دين وتاريخة واتباعه والتشكيك في الاديان الاخرى واستخدام في ذلك كافة الادوات والوسائل التكنولوجية في النص والصوت والصورة للتاثير على الجمهور حيث يسود في تلك المواقع احتكار الحقيقة المطلقة ، ويكون الفضاء الالكتروني مرتعا للانتقام من المختلف الديني والتي تنبع من ظلم اجتماعي وسياسي وكأداة للحرب النفسية.

وهناك أسباب تتعلق بخصائص وذاتية الفضاء الالكتروني وما يوفره من ميزة نسبية عن الوسائل التقليدية سواء في الانتشار، وقدرتة على صياغة الرسالة وجودتها و كمصدر للإخبار تعتمد علية الصحف التقليدية الورقية، وجاء ذلك مع حدوث عمليات تشابك للعامل الثقافي مع احتقانات داخلية تأخذ شكل تباينات اقتصادية وعرقية أو أثنية خاصة في الدول الضعيفة في بنائها القومي، ومحاولة

---

[1] B. Wellman,"Does the internet increase, decrease or supplement social capital?" <u>American behavioral Scientist</u> ,45(3),2001,pp 434-256.

الاستغلال السياسي للدين، وخاصة من قبل اليمين المتطرف في أوروبا لاثاره التمييز ضد الأقلية العربية والإسلامية أو تغليب العامل الأمني على السياسي الذي يستغل الدين في التعبئة والحشد كحالة المحافظين الجدد في الولايات المتحدة، وهناك عامل يتعلق بأهمية وتصاعد دور الدين في العلاقات الدولية وخاصة بعد أحداث ١١ سبتمبر ٢٠٠١، وزيادة انتشار تكنولوجيا المعلومات بمعدلات متسارعه والتي دفعت إلى الإحساس المتزايد بالأنا مقابل محاولة الأخر فرض قيمة ومعتقداته حيث كشفت عن الانتماءات الأولية والهويات التي كانت تعتبر سرية من قبل .(١)

وأثر الفضاء الالكتروني في القيم والافكار والاتجاهات والسلوك والمعرفة لأفراد المجتمع، وظهر دور العامل الثقافي مع وجود توترات اجتماعية بما اثر في النخب والجماعات والأفراد الذين يساهمون في صنع السياسة العالمية، والتفاعل بين كافة التيارات السياسية سواء أكانت شرعية أو غير المعترف بها ،ووجود استقطاب فكري بسعى كل جماعه فكرية للحفاظ على ما تراه موضع قدم في مستقبل جديد فهو صراع حول رؤية المستقبل.

ثالثا : جاذبية الفضاء الإلكتروني للارهابيين كوسيلة أعلام دولية

يتسم الفضاء الالكتروني كوسيلة اعلام دولية الطابع بعدة خصائص تنافسية بشكل جعلها عنصر جذب للإرهابيين والقيام بإدارة الفكرة المدركة أو التحكم بالصورة المنطبعة أي تصوير أنفسهم وأعمالهم بالضبط في الضوء والسياق الذي يريدونه، دون أن يعرقل ذلك تفحص وسائل الإعلام الرسمية لذلك التصوير أو غربلته أو تحويره (2)وقد بدأ الإرهابيون بالفعل في استخدام الفضاء الالكتروني في التأثيرعلى الرأي العام وتجنيد أعضاء جدد وجمع الأموال. وأصبحت مسالة نشر الرسالة والحصول على تغطية إعلامية إخبارية واسعة عنصرين مهمين لإستراتيجية الإرهاب، بالاضافة لوسائل الإعلام التقليدية، ويوفر الفضاء الالكتروني للجماعات الإرهابية طريقة بديلة للوصول إلى الجمهور وسيطرة مباشرة على الرسالة الاعلامية وشن الحرب النفسية والدعاية .(٣)

واستخدم الارهاب الفضاء الالكتروني كوسيلة إعلاميه تتكون من أربعة عناصر: جهاز الإرسال (الإرهابي)، والمتلقي المقصود (الهدف)، والرسالة (التفجير، الكمين)، والتغذية الاسترجاعية ورد فعل الجمهورالمستهدف، ويمارس الإرهابيين أشكالاً مكررة من استخدام اللغة المؤثرة الهادفة إلى الإقناع شفوياً وكتابياً وتصويريا ،و مما يرغم وسائل الإعلام على توفير الوصول إليها الذي بدونه لا يستطيع الإرهاب تحقيق أهدافه ،وأن كل وحدة إرهابية تتألف من أربعة أعضاء على الأقل: المرتكب والمصور وفني الصوت والمخرج. (4) وساعد ذلك الى ان اصبح الفضاء الالكتروني منبرا للجماعات الإرهابية عبر

---

(1) John Arquilla,and David Ronfeldt,. " **Swarming & the Future of Conflict.**" Rand cooperation, 2000. p 98 .

(2) Dorothy Denning, "**Information Warfare and Cyber-terrorism,**" **Women in International Security** (WIIS) Seminar, Washington, D.C. (15 December 1999).

(3) Michele Zanini and Sean J.A. Edwards, "**The Networking of Terror in the Information Age,**" in John Arquilla and David Ronfeldt (eds.), Networks and Netwars: The Future of Terror, Crime and Militancy (Santa Monica, CA: RAND, 2001, MR-1382-OSD), p. 43.

(4) بروس هوفمان،" **شكل من أشكال الحرب النفسية**"، مكتب برامج الإعلام الخارجي ، وزارة الخارجية الأمريكية، اخر زيارة للموقع (١٦-٧-٢٠٠٦) (http://usinfo.state.gov/journals/itps/0507/ijpa/hoffman.htm)

نشر رسائل الكراهية والعنف وللاتصال ببعضهم البعض وبمؤيديهم والمتعاطفين معهم من خلال الحرب النفسية التي يشنونها ، وأيضا محاوله الأفراد والجماعات مهاجمة شبكات الكمبيوتر والاتصالات فيما أصبح يعرف بالإرهاب الإلكتروني ،وليست المواقع الإلكترونية سوى واحدة من خدمات الإنترنت التي سطا عليها الإرهابيون. فهناك تسهيلات عديدة أخرى كالبريد الإلكتروني وغرف المحادثة والمجموعات الإلكترونية.

ويستخدم الكثير من هذه المواقع الإلكترونية لشن الحرب النفسية ضد الدول المعادية وقواتها المسلحة، وتعرض أفلاما مرعبة للرهائن والأسرى أثناء إعدامهم، ولاغتيال العسكريين في الميدان على يد القناصة أو إسقاط طائراتهم بالقذائف المحمولة على الأكتاف أو نسف عرباتهم باستخدام القنابل المخفية على جانب الطرق أو على يد مفجرين انتحاريين. وتحاول الرسائل الشفهية والمصورة، تثبيط عزيمة العدو وتخويفه أو خلق شعور بالذنب والشك والانشقاق الداخلي، في نفس الوقت الذي تبلغ فيه رسالة تهديد إلى الحكومات المختلفة ومواطنيها .ويحرز الارهابيون قوتهم من رد الفعل على ما قد يثيرونه من خوف لدى العدو .(1)

وكان لهذا دور كبير في تضخيم الصورة الذهنية لقوة وحجم تلك المجموعات والتي تبدأ بعدد قليل من الأفراد لديهم أو لدي أحدهم خبرة بالإنترنت وبرامج الوسائط المتعددة لبث رسالة إعلامية تخدم أهدافهم في شن حرب نفسيه ضد مستهدفيها أو الدعاية لأهدافها وأنشطتها بعيدا عن وسائل الإعلام التقليدية. أما فيما يتعلق بالطابع العسكري للإرهاب الجديد فيتم استخدام الإنترنت في التنقيب عن المعلومات، والحصول علي التمويل والتبرعات وعملية التجنيد والحشد لأتباعها ، وكذلك تحقيق الترابط التنظيمي بين الجماعات وداخلها و تبادل المعلومات والأفكار والمقترحات والمعلومات الميدانية حول كيفية إصابة الهدف واختراقه وكيفية صنع المتفجرات والتخطيط والتنسيق للعمل الإرهابي. وكذلك في تدمير مواقع الإنترنت المضادة أو اختراق مؤسسات حيوية أو تعطيل الخدمات الحكومية الإلكترونية

وشكل الإرهاب الالكتروني قاعدة للتغيير والتعبير عن الرؤى المتطرفة التي تتبني العنف بما آل إليه الإنترنت من تقسيم الجمهور إلي فئات ومجموعات صغيرة وبدأ هذا التنوع يزيد بدوره من التشتت الثقافي وذلك كإعلام فئوي يستخدم لإذكاء الصراعات العنصرية وتنمية اتجاهات الكراهية لدي الكثير من الفئات المناهضة للفئات الأخرى وتاه التوافق الثقافي الذي ميز المجتمعات القومية، وفي مقابل تلك النظرة التفتيتية للمجتمعات جاء ذلك الإعلام للترويج لرؤى عالمية ففي حين تستغله الولايات المتحدة للترويج إلي الرأسمالية والهيمنة استغله تنظيم القاعدة للترويج إلي الخلافة الإسلامية والجهاد العالمي.

وقوض الإرهاب الالكتروني من سلطة الدولة بنقل الحوادث الإرهابية للرأي العام بما يشكل خطرا نفسيا أو ضغطا علي الحكومات للمثول للمطالب السياسية التي تتبناها الجماعات الإرهابية وتهديدا لشرعية النظم السياسية الحاكمة، وعمل ذلك علي الحد من استخدام القوة في صنع القرار من جانب الدولة والتي فرض انسحابها من قطاعات إستراتيجية لصالح القطاع الخاص تحديات أمنية متزايدة،

---

(1) Karine Barzili-Nahon ," Cultured Technology : the internet and religious fundamentalism ,The information society",Taylor&Farncis group,volume21 ,number 1 , Jan –Mar. 2005 ,pp 25-40

وتطرح مسالة المواجهة الأمنية قضية حرية الرأي والتعبير عبر الإنترنت وارتباطها بالقيم الديمقراطية وكذلك مسألة الاستغلال السياسي للنظم الحاكمة لمواجهة معارضيها بشكل لا يعكس الفصل بين أمن النظام وأمن المجتمع، وفي مقابل تلك الجهود لإغلاق مواقع الإنترنت يزداد معها بالمقابل قدرة الإرهابيين على استخدام الإنترنت والفضاء الإلكتروني بشكل أكثر عمقا. [1]

ومثلت عملية التزاوج بين الإعلام والإرهاب سلاحاً ذا حدّين في شأن استخدام الإعلام الجماهيري، أحدهما (سلبي)، حيث إنها قد تكون سبيلاً لنشر الرعب والخوف على الملأ من خلال تغطيتها غير الواعية للعمليات الإرهابية وآثارها، محققة بذلك للإرهابيين هدفين هامين: (الأول): إثارة الرأي العام ولفت انتباهه إلى وجود ظاهرة الإرهاب، وإلى أن الإرهابي صاحب قضية يجب الاعتراف والاهتمام بها ومعالجتها. و (الثاني): الحصول على الشرعية الدولية لما يطالب به الإرهابيون؛ ويحرص الإرهابيون على تنفيذ عمليات مثيرة من حيث الأسلوب، أو حجم الخسائر، أو مكان وزمان وقوعها ليكون ذلك مدعاة لجذب الإعلاميين، الباحثين دائمًا وفقًا لطبيعة عملهم عن الأخبار المثيرة والهامة بالنسبة لأكبر عدد ممكن من الجماهير.أما الحد الآخر (الإيجابي) لسلاح الإعلام فيتمثل بالتغطية الواعية لقضايا الإرهابيين وعملياتهم، وفق أسلوب توعيه ينفر الرأي العام من تلك الأعمال الإجرامية، ويبرز بشاعة مرتكبيها وعداءهم للمجتمع، وسعيهم إلى التدمير والتخريب وإثارة الخوف والفزع والقلق بين الناس؛ وبذلك يكون الإعلام سلاحًا ماضياً ضد الإرهابيين.[2]

رابعا: كيفيه استخدام الجماعات الارهابيه للفضاء الالكتروني:

تستخدم الجماعات الإرهابية الفضاء الالكتروني عبر ثماني طرق مختلفة وإن كانت متداخلة أحيانا فيما بينها، [3] وهي:

١ - الحرب النفسية، من خلال نشر معلومات ملفقة وتوصيل التهديدات لنشر الرعب والصور المريعة لأعمالها عبر الفضاء الالكتروني كوسيط غير مراقب يحمل القصص والصور والتهديدات والرسائل بصرف النظر عن شرعيتها وأثرها المحتمل، وهو ما يكرس أهميتها والتهديد الذي تطرحه في مجال ممارسة هذه الجماعات للحرب النفسية .

٢ - الدعاية والإعلان عن طريق التعريف بنشاطها واهدافها حيث أضحي لتلك التنظيمات المواقع الخاصة بها، والتي تسيطر عليها وتمكنها من إعادة صياغة تصورات أنماط الجماهير إزاءها ومعالجة صورتها وصور أعدائها.[4]

٣ - التنقيب عن المعلومات، يمثل الفضاء الالكتروني وسيلة مهمة ليس لجمع المعلومات فقط بل أيضا للتنقيب عن المعلومات والتفصيلات حول الأهداف والأنشطة المحتملة، حيث يتم جمع معلومات صغيرة يتم الربط بينها لتشكل صورة اكبر لمعلومة مهمة، وكذلك الخرائط والرسوم البيانية عن أهدافها

---

[1] Gabriel Weimann," Terror on the Internet: The New Arena, The New Challenges",Op. Cit .

[2] زكريا حسن أبو دلس، مرجع سابق ذكره ص ص ٣٤-٥٦ .

[3] عادل عبد الصادق، " المتطرفون وحرية التعبير على الانترنت بين الامن والانفتاح، دراسات سياسية، جريدة الاهرام، ٢١ فبراير ٢٠٠٥.

[4] Gabriel Weimann, How Modern Terrorism Uses the Internet, The United States Institute of Peace, www.terror.net, Special Report No. 116, March 2004.

كوسائل النقل والمباني العامة والمطارات والمواني والإجراءات المناهضة للإرهاب، لتحصل علي الأقل دون الحاجة إلي وسائل غير شرعية علي٨٠٪ من المعلومات المطلوبة حول الأهداف المحتملة.

٤ ـ التمويل، حيث يتم استخدام الإنترنت للحصول علي تبرعات باستخدام التحويلات المالية عبر الإنترنت، وتدخل هذه التبرعات في حسابات جماعة قيادة وهي منظمة تكون مؤيدة بشكل واسع النطاق لأهداف جماعه ارهابية معينة هم ولكنها تعمل بشكل علني وشرعي. وعادة لا توجد بينها وبين هذا التنظيم روابط مباشرة وقد يتم استخدام منظمات عالمية ذات طابع إنساني أو خيري كمظلة لتوفير التمويل أو تعمل تحت غطائها.

٥ ـ التجنيد والحشد، حيث يتم تجديد وحشد المؤيدين للقيام بدور أكثر فعالية، من خلال الحصول علي معلومات عن المستخدمين الذين يدخلون علي مواقع هذا التنظيمات الارهابية، وتتمكن بالتالي هذه التنظيمات من الاتصال بمن تراهم أكثر اهتماما بقضايا الجماعة والأكثر ملائمة لتنفيذ أعمالها. كما يقوم المسئولون عن عمليات التجنيد بالبحث داخل غرف الحوارات والمقاهي الشبكية عن الأعضاء المناسبين من العامة خاصة ذوي المهارات التكنولوجية

٦ ـ الترابط، نظرا لأن العديد من الجماعات قد اجتازعمليات التحول من المنظمات الهرمية الصارمة التي تعمل بقيادات محددة، إلي تنظيمات فرعية لخلايا شبه مستقلة ليس لها هيئة قيادية تنظيمية واحدة، وهذه الجماعات تتمكن عبر استخدام الفضاء الالكتروني من الحفاظ علي الاتصالات مع بعضها البعض ومع أعضاء التنظيمات الأخرى، وهو ما يمكن تلك التنظيمات من إدارة أنشطتها بأسلوب لا مركزي عبر الإنترنت والتنسيق بينها أفقيا.

٧ ـ تبادل المعلومات والأفكار والمقترحات والمعلومات الميدانية حول كيفية إصابة الهدف واختراقه، وكيفية صنع المتفجرات واستخدامها.

٨ ـ التخطيط والتنسيق، حيث تستخدم الإنترنت في هذه الحالة كوسيلة للتنسيق والتخطيط سواء علي المستوي المعلوماتي أو العملياتي، فقد ثبت أن تنظيم القاعدة استخدم الإنترنت بكثافة عبر الرسائل المشفرة لتخطيط وتنظيم هجمات الحادي عشر من سبتمبر، ولضمان الحفاظ علي سرية المصدرفقد تم استخدام الإنترنت عبر أماكن الاتصال العامة.

٩- الأهداف والمضمون والرسالة: تسعي الجماعات في استخدامها للفضاء الالكتروني في مجال تحقيق البعد السياسي للارهاب من خلال التاكيد على الاهداف والمضمون والرسالة عن طريق الدعاية لأفكارهذه التنظيمات أو إنهاك قوى الدولة وإساءة العلاقات بين الدول ومحاولة استقطاب المجتمع إلى جانبها والتأثير في الرأي العام من اجل عزل النظم السياسية الحاكمة. وذلك من خلال تحقيق ثلاثة أهداف، وهي القدرة علي الوصول بمعني وجود وحدة عالمية أحادية، والسيطرة أي الإدارة البعيدة، والتنقيب أي الحصول علي المعلومات،. تستخدم أدوات أربع لتحقيق هذه الأهداف الثلاثة وهي:اولا: النقل عبر خطوط طويلة عبر الأرض و عبر الفضاء، وثانيا : الاتصالات عبر زيادة الروابط بين نقاط أكثر، وثالثا : التجميع عبر تركيز المزيد من المعلومات و ربط المزيد من المعلومات غير المتصلة، والاسترجاع بزيادة طرق استرجاع المعلومات والمعرفة.

## المطلب الثالث:

## تنظيم القاعدة والجبهه الإعلامية الإسلامية العالمية

اولا : تنظيم القاعدة وواقع دولي جديد

تميزت أحداث ١١ سبتمبر ٢٠٠١ بأنها جاءت من داخل الولايات المتحدة ولم تأت عبر الحدود الدولية، وكان الفاعلون مختلفين في الانتماء للدول ولهم مؤيدون من دول عديدة، ومعظم من قاموا بها قد تعلموا داخل الولايات المتحدة ويحملون الجنسية الأمريكية، ولم يكن الهدف عسكريا بل كان الهدف هو إصابة رمز من رموز الهيمنة الأمريكية، وجاءت تلك الأحداث بضحايا ليس فقط أمريكيين، وأصبح هناك سياسة أمنية جديدة تتجاوز الفصل التقليدي ما بين المستويات الدولية والمحلية للأخطار والتي كانت أساس الفكر الأمني التقليدي.(١)

و كشفت تلك الاحداث قدرة تنظيم القاعدة على التعامل مع وسائل التكنولوجيا حيث تم التخطيط والتنفيذ لها بالاعتماد على جزء كبير من التكنولوجيا المعلوماتية ووسائلها، والتي تضمنت ما يمكن أن نطلق علية أسلحة افتراضية من نوع خاص، فكان الكمبيوتر وبرامجه والبريد الالكتروني ونظم محاكاة الطيران Flight Simulator وأجهزة المحمول والرسائل القصيرة SMS وشبكات الإنترنت وأجهزة الصرف الآلي ATM والتحويلات المالية عبر الإنترنت والمساعدات الرقمية الشخصية Personal Digital Assistant بالإضافة إلى كمبيوترات الجيب Hand Held وهذا ما يشكل صورة إرهاب جديد يطلق علية الإرهاب الإلكتروني أو الشبكي Cyber Terrorism. (٢)

وكان تنظيم القاعدة هو أول حركه تمارس نشاطا إرهابيا بالانتقال من الفضاء الأرضي إلى الفضاء المعلوماتي والإنترنت ولتنتقل من منظمة عاملة إلى منظمة دعاية وأصبحت شبكة الإنترنت وسيلة تعبير واتصال شائعة الاستخدام بين المتطرفين الإسلاميين في كل من العالم الإسلامي والأقليات الإسلامية المهاجرة في الغرب. وليس من الصعب معرفة السبب الكامن وراء هذه الشعبية الفائقة للإنترنت وسط الأصوليين والمتطرفين الإسلاميين، فالإنترنت يوفر مساحة حرة للاتصال، تربط ما بين الجماعات الإسلامية المتعددة . (٣)

وقد دفع ذلك الاستغلال من جانب تنظيم القاعدة لشبكة الإنترنت إلى لجوء الولايات المتحدة لغلق المواقع التي تراها توفر معلومات أساسية عن صنع القنابل أو أساسيات صنع القنبلة الذرية أو تفصيلات المرافق الحيوية وخرائطها وذلك منعا من استغلال ذلك في التنفيذ لعمل إرهابي. (٤) ويستخدم الجهاديون

---

(1) Brynjar Lia," **Globalization and the Future of Terrorism: Patterns and Predictions,** Routledge, London,UK, 2005,pp23-243.

(2) وقد ثبت استخدام خالد شيخ محمد المتهم الرئيسي في أحداث ١١ سبتمبر ٢٠٠١ ما يسمى "بالقنطرة الخفية" على الإنترنت لمنع كشف الرسائل الالكترونية عن طريق فتح حساب في الهوت ميل Hotmail أو غيرها حيث يتم حفظ الرسالة كمسوده بالايميل بدون إرسالها، ويتم تبادل كلمة المرور من خلال المنتديات أو الدردشة، بذلك لا يتم إرسالها ويصعب مراقبتها، أو استخدام عدد من الرسائل غير المرغوبة للتغطية على رسالة واحدة وهذا ما جعل هناك صعوبة في جمع المعلومات الاستخباراتيه.خاصة مع افتقاد أجهزة المخابرات الأمريكية لكوادر تتقن اللغة العربية.

(3) Timothy L. Thomas , "**Al Qaeda and the Internet: The Danger of "Cyber planning"** From Parameters, Spring 2003, pp. 112-23.

(4) Gabriel Weidman, How Modern Terrorism Uses the Internet,Op.Cit.

ثلاث وسائل للمساعدة في تنفيذ اهدافهم عبر الفضاء الالكتروني الأولى هي المنتديات وهي بمثابة مساحات مفتوحة للمشاركة. ويمكن للشخص من خلال مشاركته فيها أن يصبح قادراً على نشر رسائله وأفكاره وبالتالي فإن بعضها يتم استعماله لنشر بيانات القاعدة"، أما الوسيلتين المتبقيتان فهما "الدردشة Chat، التي باتت تستعمل كوسيلة للتجنيد الفكري والعسكري" و"الغرف الصوتية"، التي تسمح للمشاركين فيها بالتواصل صوتياً على شبكة الإنترنت. وأصبحت القاعدة، التي كانت تدون في السابق كل تقاريرها وبياناتها، باتت تستعمل النظم المعلوماتية وتنشر على الإنترنت "كتباً الكترونية" تشرح عقيدتها "من أولها إلى أخرها"، وتنشر طرق تصنيع المتفجرات بواسطة مواد كيميائية متوفرة في الأسواق."[1]،

ومنذ أحداث الحادي عشر من سبتمبر ٢٠٠١ تضاعفت أعداد المواقع التي تمارس "الجهاد الالكتروني" بشكل كبير، وتمكن الموصوفون بالأصوليون والإرهابيون من إيصال ونشر إخبارهم في المواقع والمنتديات وغرف الدردشة، بل أنهم تمكنوا من إنشاء مواقع خاصة بهم تنشر أفكارهم، كما أنها تنشر محتويات تسجيلات وخطب وصوراً لعمليات ضد قوات الاحتلال في العراق وفلسطين، مما جعل "الأصوليين الإسلاميين"من بين اكبر المستفيدين على الإطلاق من ثورة المعلومات والاتصالات التي يشهد العالم تسارعا كبيرا في نموها. ولا تخلو "مواقع الجهاد الالكتروني" من مواد تعلم روادها فنوناً قتالية، بل وترشدهم إلى كيفية صناعة القنابل وغيرها من وسائل القتال،

وتحتضن شبكة الإنترنت مجموعة من المواقع المتطرفة ذات التأثير والشعبية الكبيرة والتي يسيطر عليها هاجس الجهاد والحرب المقدسة ضد الكفار، والتي وصلت الى ٤٨٠٠ موقع وفق مصادر غربية ، و من الصعوبة بمكان أن تتبين في هذه المواقع أن الهدف بعيد المدى المفترض لدى الإسلاميين، وهو إقامة الدولة الإسلامية؛ لفرط تركيزها على الجهاد فقط. وبدلا من هذا تعرض هذه المواقع مؤلفات وأدبيات ضخمة تتحدث عن الجوانب الفقهية والعملية والفنية للجهاد.

وهناك مواقع توفر كتابات نظرية متنوعة واجتهادات فقهية لكبار منظري التيارات الجهادية، أمثال الأردنيين "أبو مصعب الزرقاوي" و "أبومحمد المقدسي". وتبرز كذلك كتابات المصري "سيد إمام شريف"، ومن بينها مجلد "الجامع في طلب العلم الشريف" الذي يتجاوز الألف وستمائة صفحة من القطع الكبير، والذي يتناول جوانب فكرية متعددة عن الإسلام السلفي المتشدد، بالإضافة إلى كتاب آخر مخصص للجهاد فقط بعنوان "العمدة في إعداد العدة" يتألف من مئات الصفحات أيضا. وهناك فئة منفصلة من الكتابات الغزيرة مخصصة للتصدي والرد على الشيوخ والإسلاميين المعتدلين الذين يعارضون الجهاد كليا أو جزئيا.

ومن وجهة نظر المتطرفين فإن هؤلاء الإسلاميين المعتدلين المنفتحين خونة، لأنهم يرونهم متعاونين مع الكفار لصرف المسلمين عن الإسلام الحقيقي الذي يمثلونه. وهناك مواقع أخرى تركز على الجوانب العملية والفنية للجهاد؛ فيمكن أن يجد الفرد كتيبات تحوي تفاصيل عن إنتاج المتفجرات والسموم،

---

[1] Ibid.

وأيضا عن القضايا الخاصة بأمن الجهاد والمجاهدين مثل كيفية حفظ الأسرار والتعامل مع المحققين في حال القبض على أي عضو او ناشط وطرق التدريب على الجهاد تحت ظروف مختلفة.

ويحوي أحد هذه المواقع كتابا عن تمرينات اللياقة البدنية للنساء المجاهدات وفي المنتديات وغرف الدردشة الإسلامية المتطرفة يتم تبادل وجهات النظر، ومناقشة الموضوعات العملية المتعلقة بالجهاد، إضافة للفتاوى حول الجهاد وغيره من القضايا الإسلامية من قادة الحركات الجهادية وفقهائها حول أسئلة مثل: "وجهة نظر الإسلام في الذهاب للجهاد من دون إذن الوالدين"، و"حكم الإسلام فيمن يعمل إماما بمسجد يُموّله الكفار".

ويُعد الإنترنت كذلك وسيلة يُنشر من خلالها المئات من الأشرطة المسموعة والمرئية التي تحوي مواعظ دينية لمشاهير الوعاظ، كما تضم أشرطة عمليات عسكرية جهادية، فالكثير من العمليات في العراق وأماكن أخرى تسجل على أشرطة فيديو، وتُبث على الإنترنت، بما فيها أشرطة تتضمن صورا لأشخاص يتم ذبحهم وفي بعض الأحوال تصل هذه المنتجات السمعية والبصرية إلى درجة شبه احترافية من الجودة، مثل ما تفعله شركة "سحاب" التي تنتج أشرطة فيديو لـ "أسامة بن لادن" وكثير من الهجمات الإرهابية والتفجيرات في المملكة العربية السعودية. أكثر من أربعة آلاف موقع الكتروني لها علاقة بالنشاطات الإرهابية، ويعتقد أن هذه المواقع تمتلك القدرة على التوالد، وقد قامت مجموعة تابعة لمنظمة "القاعدة" عبر موقع Al-Jinan.Org بتطوير برنامج "الجهاد الإلكتروني" ElectronicJihad الذي يسمح لجميع مستخدمي الإنترنت، حتى ولو كانت معلوماتهم التقنية صفرا، أن يقوموا بشنّ الهجمات على قائمة من المواقع المخزنة فيه، والتي يتمّ تحديثها بشكل دوريّ.

ويقوم البرنامج بمحاولة إيقاف عمل الأجهزة الخادمة للهدف، وذلك للتأثير في اقتصاده، خصوصا إن كان الموقع في داخل الولايات المتحدة الأميركيّة التي تعتمد البنى التحتيّة فيها على القطاع الخاصّ بشكل كبير جدًا، ولذلك فإنّ إيقاف عمل شركات محدّدة يعني التأثير السلبيّ في اقتصاد البلد، ويحتوي البرنامج على واجهة تفاعل سهلة جدًا، ويمكن فيه اختيار سرعة الهجمات وسرعة الإنترنت لدى المستخدم، بالإضافة إلى قدرته على تجاوز تقنيات الحجب الموجودة في بعض البلدان وأفسح هذا البرنامج المجال أمام عدد كبير من المستخدمين غير التقنيين بشنّ الهجمات على مواقع تراها المجموعة معاديّة لمبادئها. وتوفير "الأسلحة"، وتعليم تقنيات الهجمات الإلكترونيّة، وكيفية شنّ هجمات كبيرة في وقت واحد لإلحاق أكبر قدر ممكن من الضرر، وبما يؤدي لتوقفه عن العمل بشكل غير طبيعيّ، وانخفاض سعر السهم للشركة بسبب الخوف من فقدان معلومات سريّة أو خاصّة.[1] وتمكن تنظيم القاعدة من تشكيل العديد من المنابر والمواقع مثل شبكة الإخلاص ومنتديات السحاب والنداء وتم إعلان تنظيم القاعدة مؤتمرا صحفيا هو الأول من نوعه عبر الإنترنت مع القيادي الثاني أيمن الظواهري حيث امتدت فترة تلقي الأسئلة من ١٦ ديسمبر٢٠٠٧حتى يناير ٢٠٠٨ وذلك في إطار نشاط الجبهة الإعلامية الإسلامية ومؤسسة سحاب الذراع الإعلامي لتنظيم القاعدة.

---

[1] جريدة الشرق الأوسط ٢٤- ٧- ٢٠٠٧ .

وبرزت قدرته في استخدام أجهزة الكمبيوتر والإنترنت والتي تتميز بعده خصائص أهمها : فكرة الإنترنت القائمة على التشبيك وشبكات فرعية وقيادة وسيطرة أحادية توجد في إدارة الشبكة في الولايات المتحدة حيث مثل ذلك تقاربا فكريا مع هيكل التنظيم وخلاياه وقيادته ، ومكنت تنظيم القاعدة من التواصل مع الجاليات العربية والإسلامية بما مثل خرقا استراتيجيا للأمن الأوربي والغربي ،واستغلال مشاكل التمييز والتهميش ضد هذه الجاليات والسياسات الرأسمالية للدول الكبرى وبعض القوى التي ترحب بشكل غير معلن بإنهاء النفوذ الأمريكي لإفساح المجال لها.

واستغل تنظيم القاعدة حرب العراق والمعارضة الدولية بشأنها في تفعيل دورة خاصة في عملياته العسكرية في العراق لأعاده فكر المقاومة في مقابل الاحتلال لاكتساب مزيد من الشعبية مع افتقار الإنترنت إلى الحدود القومية والمحددات الثانية يتوافق تماما مع رؤية أسامة بن لادن لتنظيم "القاعدة" الذي أسسه بغرض إثارة التمرد وسط "الأمة" الإسلامية وأحاط نفسه بأتباع ينحدرون من أصول عرقية متباينة، وبهذا الطموح أصبحت الإنترنت مكان التقاء لطوائف متنوعة من المتطرفين، كما أصبح "ملجأ افتراضيا" لشبكة "القاعدة" على المستوى الدولي. ويعتقد "جون آركيلا"، الأستاذ بمدرسة البحرية للدراسات العليا ومبتكر مصطلح "حرب الإنترنت" منذ أكثر من عشر سنوات، إن شبكة "القاعدة" والجماعات التابعة لها "أدركت إن شبكة الإنترنت قد تجاوزت الزمان والمكان في الكثير من الجوانب، وأصبح إن لجوء شبكة "القاعدة" للعمل عبر شبكة الإنترنت له أثارا سلبيه على مقدرات أجهزة الأمن الأميركية على توجيه ضربة لها وهي في اضعف حالاتها أي وهي في حالة حركة ."[1]

ومع المواجهة مع تنظيم القاعدة الذي انتقل نشاطه الى السودان مطلع عقد التسعينات ثم اضطر للخروج لليمن قبل العودة مجددا إلى أفغانستان للتدريب وأصبحت عملية التنقل والسفر أمراً ضروريا لعناصر "القاعدة" وهم لا يضطرون إلى حمل إي شيء أو يتركوا دليلاً يمكن أن يتسبب في إدانتهم، فهم ليسوا في حاجة إلى حمل إرشادات أو خطط أو وصفات مكتوبة على الورق، إذ إن كل هذه المواد يمكن أن ترسل مشفرة عبر شبكة الإنترنت إلى الجهة المعنية ضمن ملايين الرسائل التي يعج بها عالم الإنترنت، وبالنسبة إلى مواقع تنظيم القاعدة فقد تبنت إستراتيجية (الملابس البديلة) Alternative Clothes ، وأن يكون هناك بدائل للموقع، جاهزة للاستخدام في حالة إغلاق أو تعطيل الموقع الرسمي، وأيضا بدائل لاسم الموقع (الدومين)، وبدائل لشركة الاستضافة، وبدائل للملفات، بحيث يظهر الموقع، في حالة تدمير أو إغلاق الموقع، من جديد وبسرعة، وكأن شيئا لم يحدث[2] وهذا ما جعل تنظيم القاعدة يعمل بشكل أفضل من الإدارة الأمريكية لكسب مزيد من التعاطف العالمي في الحرب الدائرة بين الجانبين على مواقع شبكة الإنترنت [3]. وتوازت المواجهة العسكرية بمواجهه مثيلة في الفضاء الإلكتروني والذي استخدم كبيئة وساحة إعلامية للترويج للرأسمالية والهيمنة الأمريكية في مقابل ترويج تنظيم القاعدة للخلافة الإسلامية والجهاد العالمي ومن خلال متابعة خبرة سنوات مكافحة

---

(1) كما يرى ذلك "مايكل شوير" المسئول السابق عن وحدة وكالة الاستخبارات المركزية الأميركية المكلفة بتعقب أسامة بن لادن.

(2) عمر عبد العزيز مشوح،" إستراتيجية (الطين) الصهيونية لتطويق المواقع الإسلامية"، مرجع سابق ذكره
(http://www.alasr.ws/index.cfm?method=home.con&ContentId=8500)

(3) جريدة الحياة اللندنية ٢ فبراير ٢٠٠٨ .

الإرهاب الأمريكية يتضح أن التركيز علي العامل الأمني فقط قد أدي إلي نتائج عكسية فعندما انطلقت الطائرات الأمريكية لضرب أفغانستان انطلقت معها حركة تنظيم القاعدة علي الإنترنت والمنظمات الأخرى الحليفة له لتكتمل تلك الحلقة باحتلال العراق ليكتسب تنظيم القاعدة أرضا جديدة لبث أفكاره التنظيمية المعادية للولايات المتحدة وللغرب.

وانتقلت ساحة المواجهة الأمريكية مع تنظيم القاعدة في إطار حرب أفكار متبادلة وتنافسا حول جمهور عالمي واسع يستقبل الرسالة الإعلامية علي شبكة الإنترنت والتي أصبحت مصدرا للأخبار للعديد من وسائل الإعلام.[1] وفي حين ركزت الإدارة الأمريكية جل اهتمامها علي عملياتها العسكرية فان تنظيم القاعدة ركز بصورة اكبر علي الجانب الإعلامي من عملياته كجزء من المواجهة وحتى سياسة حجب المواقع التابعة لتنظيم القاعدة لم تؤد إلا إلي توالد العديد من المواقع الأخرى بشكل اقترب فيه تنظيم القاعدة من النجاح إعلاميا ومخاطبة الغرب والعمل علي عزل القيادات الأمريكية وحلفائها عن شعوبها بتكوين إعلام آخر مختلف عما تروجه وسائل الإعلام الأمريكية للشعب الأمريكي وخلق شبكة مؤيدين عالميين عبر الخلايا النائمة في العالم.

ففي رسالة لأيمن الظواهري إلى الزرقاوي قال "إننا نخوض أكثر من نصف معركتنا في الساحة الإعلامية". وجاء ذلك عبر توظيف الفضاء الالكتروني كوسيلة اعلام قادرة للتعبير عن المسائل العقائدية والثقافية والتعليق على الاحداث الجارية وتشكيل رسالة اعلامية متكاملة ،ومثل الفضاء الإلكتروني ساحة أخرى للمواجهة مع الولايات المتحدة وتنافسا حول السيطرة والتأثير على الرأي العام الدولي وكسب تعاطفه، وتارة أخرى يتم استخدامه لدعم الأنشطة الإرهابية والترويج لها ومحاولة ربط التنظيم تلك الأنشطة تحت إطار المقاومة ضد قوات الاحتلال الأمريكي لاكتساب مزيد من الشعبية [2].

ثانيا : تنظيم القاعدة و الجهاد الالكتروني

تظهر الأهداف التي نشرت على شبكة المجموعات الجهادية الإلكترونية أن الدوافع العقائدية التي تحرك "المجاهدين" على شبكة الانترنت هي نفسها التي تحرك "المجاهدين" على خطوط المواجهة الأمامية ، وأنهم يعتبرون أنفسهم "مجاهدين في خدمة الإسلام " ونشر كلمة التوحيد عبر شبكة الانترنت، التي يرونها ساحة قتالهم التي من خلالها يمكنهم هزيمة الغرب بشكل فعال. فهم ليسوا مثل القراصنة الآخرين الذين هدفهم الأذية فقط أو حب الظهور أو أية أهداف دنيوية أخرى. والتي قد يتم استخدام الاخيرة كوسيلة وليست غاية في مهاجمة من يرونهم عنصريين، ومواقع الأمريكيين والشيعة وكافة المواقع التي يرونها فاسدة على الشبكة .،و أحد أهداف الجهاد الإلكتروني الذي يمارسه" المجاهدون" هو مساعدة الإسلام والقضاء على المواقع التي تهاجم الإسلام ،والانتقام للشهداء والأسرى من "المجاهدين" ورفع معاناة المسلمين" عبر اختراق شبكاتهم الالكترونية والعمل على إنزال الضرر

---

(1) راسم محمد الجمال "نظام الاتصال والإعلام الدولي :الضبط والسيطرة ،الدار المصرية اللبنانية ،القاهرة ،٢٠٠٥ .

(2) Graham E. Fuller, Islamist Politics in Iraq after Saddam Hussein, The United States Institute of Peace, Special Report No. 108, August 2003.

بمعنويات الغرب والسعي لإنزال أكبر ضرر اقتصادي ممكن والذي يعد بملايين الدولارات من الخسائر.ودفع الغرب إلى حافة الانهيار الكامل ، و مهاجمة وتعطيل بعض المواقع الحيوية وانعكاس ذلك على الاقتصاد العالمي وأسواق البورصة التي تعتمد في ممارسة نشاطها اعتماداً كلياً على شبكة الاتصالات الالكترونية.

ثالثا :الجبهة الاعلامية الاسلامية العالمية :

تنقسم الجبهه الى عدة اقسام منها اقسام الاعلام الفني والتقني والبريدي والسمعي والمرئي والترجمة والنشر والتوعوي والكتب والنشرات ، و يحدد تنظيم القاعدة مهمه الجبهة الإعلامية الإسلامية العالمية بانها مؤسسة إعلامية كبيرة واسعة الانتشار ولا يحدها حد ، هدفها تبيان الحقائق بأساليب منطقية وشرعية ونصرة الإسلام والمسلمين والدفاع عن الإسلام والدعوة إليه ، و هي بمثابة قاعدة الإعلام الإسلامي على شبكة الإنترنت، والجبهة هي رسول المجاهدين إلى أبناء الإسلام ولغير المسلمين الذين لا يعادون الإسلام والمسلمين بأي شكل من الأشكال،، و يندرج تحت الجبهة عدة جهات إعلامية على الإنترنت، سواء كانت منتديات أو مواقع أو مجموعات بريدية أو مؤسسات إعلامية متنوعة.[1]

وتصف الجبهة نفسها بانها ليست ملكا لأحد، فهي ملك لكل المسلمين الغيورين، وأن ليست لها حدود جغرافية.،و لا تتبع الجبهة لأي حزب أو جماعة أو تنظيم معين، وللجبهة قيادة عامة ورمزية ، يكمن دورها في التحريض والحث والتشجيع على كل ما ينفع المسلمين ويرقى ويسمو بالإعلام الإسلامي خصوصا على شبكة الإنترنت.،وتحرص الجبهة على مواكبة التطور فيما يخص البرامج والتطبيقات التي يستعملها الإعلاميون ،و إقامة الدورات ونشر الإرشادات الإعلامية. وتحرص الجبهة على مشورة أهل الخبرة في مجال الإعلام. وتؤكد انها تنطلق من منطلقات إسلامية وأخلاقية منبثقة من الكتاب والسنة وإجماع العلماء، ولا تحبذ الفرقة والتعصب والخلاف، وان قيادة الجبهة لها مرجعية شرعية . وتستخدم الجبهة كل الأساليب بالصوت والصورة وبالمقال والشعر و الإصدارات الفلاشية وغير ذلك ، ونشر كل ما ينتج والتنسيق مع الجماعات "المجاهدة" . وتؤكد الجبهة انها تحترم وتقدر كل الآراء والأذواق والمشارب ما دامت لاتخالف أحكام الشريعة الغراء ولا تخرج عن الأصول والثوابت.،وتمنع الجبهة كل من ينضم تحت لوائها القذف والشتم والسب وغير ذلك من الأخلاق السيئة التي تخالف تعاليم الإسلام.،ومن حق الجبهة إصدار رسائل تحذير وتنويه سواء بالصوت والصورة والبيان المكتوب والمسموع، لكل من يشوه سمعة المجاهدين والدعاة والعلماء والمسلمين العاملين لدينهم وأمتهم.،و للجبهة وكلاء وناطقين باسمها في المنتديات والمواقع الإلكترونية.

ويصدر عن الجبهه العديد من الاصدارات السمعية والبصرية ومن اشهرها مجله صدى الجهاد ومؤسسة السحاب ومنتديات الفردوس الجهادية والاخلاص والانصار وصوت الجهاد وغيرها وتتميز تلك المنتديات بقدرتها على التخفي ومواجهه محاولات الحجب والمطاردة من جانب الولايات المتحدة او حلفائها ،كما تتميز بارتفاع ملحوظ في قدراتها وتطورها التقني

---

(1) للمزيد حول الجبة واقسامها المختلفة يمكن زيارة احد المنتديات على الرابط التالي (اخر زيارة ٢-٦-٢٠٠٧) (http://www.paldf.net/forum/showthread.php?t=38603)

## المبحث الثالث:

## طبيعة وانماط استخدام الفضاء الالكتروني في الصراع الدولي

يمكن القول ان تعرض الفضاء الالكتروني لانماط الحرب والصراع يمكن ان يتم تصنيفة الى صراع مرتفع الشدة واخر صراع منخفض الشدة،وعلى الرغم من ان العالم لم يشهد تحول الفضاء الالكتروني الى ساحة وحيدة بين الدول الا انه جاء موازيا للحرب التقليدية كما حدث في حالة الحرب الجورجية الروسية في اغسطس ٢٠٠٨ وربما يصل الى ذلك في المستقل ، بينما جاءت الحرب منخفضة الشدة بصورة مستمرة ودائمة والتي تعبرعن صراعات اعمق واكثر امد وترتبط بالصراعات ذات الطبيعه المعقدة والمتداخلة ،و أصبح الفضاء الإلكتروني ساحة لنقل الصراعات وتصفية الخلافات بكافة انواعها بين الفرقاء ،و فرضت نفسها بقوة على واقع الصراعات المسلحة وغير المسلحة،وزادت التقنيات الرقمية ومدى التقدم العلمي بها من اضفاء درجة الفاعلية على ذلك النوع من الحروب عبر الفضاء الالكتروني. ويقوم الباحث باستعراض ذلك من خلال ثلاثة مطالب يتعلق الاول باستخدام أسلحة الفضاء الالكتروني في الصراع الدولي،والمطلب الثاني: هجمات الإرهاب الالكتروني ونمط الحرب الباردة والصراع منخفض الشدة ،والمطلب الثالث: هجمات الإرهاب الالكتروني و نمط الحرب الساخنة والصراع مرتفع الشدة.

### المطلب الأول:

### استخدام أسلحة وهجمات الفضاء الإلكتروني في الصراع الدولي

كما هو الحال في أية حرب، فإن الجيوش المتصارعة تستهدف دوما ثلاثة عناصر أساسية من أجل كسب المعركة؛ وهي العناصر العسكرية، والاقتصادية، والسياسية أو بكلمات أخرى إرادة الخصم، وفي عالم حروب المعلومات تجد العناصر الثلاثه ذاتها وعلى رأسها مراكز القيادة والتحكم العسكرية، والبنوك والمؤسسات المالية، ومؤسسات المنافع كمؤسسات المياه والكهرباء وذلك لإخضاع إرادة الشعوب. وإذا قامت دولة بتدمير شبكة الإنترنت بشكل متعمد، فإن دولة أخرى قد تعتبر هذا الأمر عملا عدائيا، وقد لا يكون الهدف هو تدمير الشبكة كليا أو تعطيلها حيث أنها تساعد حتى الطرف المعتدي في مراقبة المحادثات بين الأعداء أو نشر معلومات خاطئة حيث يعتبر ذلك فرصة استخباراتي مذهلة، كما أن استخدام الإنترنت من اجل السيطرة على المعلومات يمكن أن يعود بفائدة اكبر من تعطيل الشبكة نفسها أو تعرضها للهجوم ، عندما يتعلق الأمر بالإستراتيجية العسكرية والعمل على إضعاف إرادة المحاربين وشن حرب نفسية والتحكم في المعلومات.[1]

أولا : الإرهاب الإلكتروني و الهجوم المسلح

تعد هجمات شبكات الكمبيوتر والتي يطلق عليها حرب الفضاء الإلكتروني تعد جزءاً من عمليات المعلومات والتي يمكن أن يتم استخدامها في مستويات ومراحل الصراع المختلفة سواء أكان على الجانب التكتيكي أو الاستراتيجي أو العملياتي، ويتم استخدام تلك الهجمات في أي وقت سواء أكان وقت سلم أم حرب أم أزمة، وتعرف كليات الحرب الأمريكية الإرهاب الإلكتروني، وتدعوه بهجمات

---

(1) Rebecca Grant,"**Victory in Cyberspace**", The Eaker Institute, the policy and research arm, The Air Force Association of US , October 9, 2007 (www.afa.org/media/reports/victorycyberspace.pdf -)

الشبكات الكمبيوترية، وتصنفه تحت بند "العمليات الإلكترونية".(1) ويتضمن التعريف أن الحرب الرقمية هي "الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها." (2) وأنه العمليات الإلكترونية التي تتضمن أنشطة مثل أمن العمليات والعمليات النفسية والخداع العسكري والهجمات الفيزيائية والهجمات على شبكات الكمبيوتر وتوجد طرق عديدة يمكن من خلالها تنفيذ الهجمات عبر الفضاء الالكتروني، منها الهجمات المباشرة من خلال التدمير الفيزيائي لأجهزة الخصم، أو نقاط الاتصالات الهامة ضمن شبكاته، وذلك باستخدام القوة العسكرية المباشرة. وهناك أيضا سرقة المعلومات من أجهزة الخصم، ومن ثم اتخاذ قرارات أفضل في المعركة، إضافة إلى تخريب قواعد بيانات الخصم والتلاعب بها، لجعل الخصم يخطئ في اتخاذ القرارات. وبالطبع هناك استخدام الفيروسات والاساليب الالكترونية مثل هجمات الحرمان من الخدمات للتأثير على مواقع الخصم، مما يؤدي إلى التقليل من مقدرة الخصم على الاتصال وإبطاء قدرته لاتخاذ القرار.

وتتضمن هجمات الكمبيوتر حدوث هجوم على خطوط الاتصالات وتأتي تلك الهجمات من مسافة بعيدة عن مصدر الهجوم وذلك عبر الشبكات الدولية للمعلومات العابرة للحدود ومن خلال موجات الراديو أو الشبكات الدولية للاتصالات بدون تدخل مادي أو طبيعي في الأراضي الخاصة بدولة أخرى أو القيام بغزوة تقليدية، وعلى الرغم من الاستخدامات الحديثة لهجمات الفضاء الإلكتروني في الصراعات الحديثة في عصر المعلومات إلا انه لم يتم إدماجها بشكل كامل في العقيدة العسكرية للجيوش الحديثة، وان كان يعد بداية لأخذها في الاعتبار في سبيل الاستحواذ على القوة وامتلاكها من خلال تطوير أسلحة الفضاء الإلكتروني لكي يتم استخدامها في حروب المستقبل وبما ينطوي علية تغيير المبادئ الخاصة بشن الحرب وميدان الحرب والطرق والوسائل الحربية المتاحة، وهي هجمات يمكن أن تحدث سواء في أوقات السلم أو الأزمات الدولية.

ثانيا: أسلحة الفضاء الإلكتروني كعنصر في القوة العسكرية

ظهر الفضاء الإلكتروني كأحد مجالات الحرب مثل الجو و الفضاء الخارجي و الأرض و البحر، وأصبح الفضاء الإلكتروني يستخدم مجال للاستخدام العسكري وغير السلمي، وقد لا تؤدي الحرب في الفضاء الإلكتروني إلى مأساة الكترونية بالضرورة بل إلى فرض نوع من السيطرة على مجرى الأحداث في العالم وفق مصلحه من يقوم بها على جبهة واسعة النطاق من السهل الاختفاء بها، كما إن أثار الهجوم قد لا تتساوى مع تكاليفه مع صعوبة تحديد هوية مصدر الهجوم، الذي يصدر من جانب واحد مما يجبر ضحايا الهجوم على اتخاذ وضع الدفاع، وعدم قدرتهم على شن هجوم مضاد وان حدث

(1) Jennie M. Williamson, **Information Operations: Computer Network Attack in the 21st Century.** Carlisle Barracks, PA, U.S. Army War College, 2002. pp 22-25..Also available online at: (http://handle.dtic.mil/100.2/ADA402018)

(2) Michael Wynne," Flying and Fighting in Cyberspace", Space Power Journal &Air, fall 2007 , pp1-11, ( http://www.airpower.au.af.mil/apjinternational/apj-a/2007/fal07/wynne.pdf)

يكون تأثيره محدود لعدم معرفة مصدر الهجوم.[1] وكانت المعلومات والمعرفة على مدار التاريخ البشري قد لعبت دورا هاما وحيويا في تشكيل القوة فان التطور السريع لتكنولوجيا الكمبيوتر وخاصة في الشبكات قد أحدث تحولا كبيرا في مفهوم القوة ترتب عليه دخول المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء الالكتروني دورا اساسيا في تعظيم القوة واستحواذها، وكنتيجة مباشرة لذلك أصبحت القدرة التي أتاحتها التكنولوجيا الحديثة للدول تستخدم تعظيم إمكانياتها في امتلاك أدوات حرب المعلومات وتقنياتها في ترسانتها العسكرية.[2]

وجعل الفضاء الالكتروني لأي فرد في المجتمع الدولي في موقع الاستفادة من منافعه واستخدامه للتفاعل المباشر مع غيره إلى جانب ظهور الاستخدام غير السلمي له، وشكل ذلك تأثيرا هاما على السلام والأمن الدولي وعلى التنمية الاقتصادية في العالم خاصة مع استخدام تلك المعطيات من جانب الفاعلين من غير الدول وازدياد توظيف الفضاء الالكتروني كأفضل الوسائل لتحقيق أهدافهم الخاصة [3]، وأصبحت عملية التفوق في مجال الفضاء الإلكتروني يتيح تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء، وتعتمد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة، وأوجدت ملايين أجهزة الكمبيوتر المنتشرة حول عالما افتراضيا نشأ نتيجة عملية الاتصال و مثل وسيطا جديدا للقوة حيث يمكن للقراصنة دخول الفضاء الإلكتروني ومحاوله السيطرة على الاجهزة وسرقة المعلومات وإفسادها أو تعطيلها بما أصبحت المجتمعات والجيوش الحديثة تعتمد اعتمادا كبيرا على أجهزة الكمبيوتر ويعرضها للخطر، ومما جعل الإنترنت مرادفا لاستخدام الذكاء الاصطناعي [4].

وظهرت اسلحة الكترونية جديدة ومتعدده كالفيروسات وهجمات انكار الخدمة والاختراق وسرقة المعلومات والتشويش، وتلعب مثلاً القنابل الإلكترونية دور في تنفيذ عدد من المهام الإستراتيجية مثل تعطيل الاتصالات والتشويش عليها والتنصت على المكالمات، وبث معلومات مضللة عبر شبكات الحاسب والهاتف، ومنها تقليد بصمات الأصوات وخاصة أصوات القادة العسكريين وعن طريق ذلك يمكن إصدار أوامر ضارة بالقوات، واستهداف شبكات الحاسب بالتخريب عن طريق نشر الفيروسات ومسح الذاكرة الخاصة بالأجهزة المعادية، ومنع تدفق الأموال وتغيير مسار الودائع، وإيقاف محطات الكهرباء عن العمل وقد صممت لذلك قنبلة إلكترونية خاصة أطلق عليها اسم"cbu94"تنطلق منها عدة قنابل في الجو وتستهدف محطات الكهرباء وتؤدي إلى احتراقها وتدميرها بالكامل، وفي حرب الخليج الثانية تم ابتكار العديد من الأسلحة الهجومية الإلكترونية وخاصة تلك المعتمدة على الطاقة الموجهة الحديثة - ومنها أسلحة الميكروويف عالية القدرة (High-power Microwave Weapons) والمعروفة

---

(1)Kevin G. Coleman, A Cyber War has begun, Cyber Warfare, The Technolytics Institute, September 2007(http://www.technolytics.com/Technolytics_Cyber_War.pdf)
(2) Dimitrios Delibasis," State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century", Peace Conflict and Development: An Interdisciplinary Journal, Issue 8, February 2006, available from (http://www.peacestudiesjournal.org.uk)
(3) Characteristics of Information Superiority', Enabling Operations– Information Superiority, FM3-0 Chapter 11,2004 (http://www.iwar.org.uk/iwar/recources/fm3-0/chapter11.htm)
(4) Martin C. Libicki," Conquest in Cyberspace National Security and Information Warfare", Cambridge University Press, RAND Cooperation, California, 2007 pp.100,124,166,215,230,285,306

اختصارا بـ(HPM) وهي من أهم الأسلحة الجديدة في مجال الحرب الإلكترونية، ويمكن استخدامها لاختراق الأهداف عالية التحصين لتدمير و"شل"أسلحة الدفاع الجوي والرادارات وأجهزة الاتصال والحاسبات التي تعمل ضمن منظومة القيادة والسيطرة.

ويمكنها تدمير أجهزة التحكم في إنتاج وتخزين المواد الكيماويةوالحيوية، وتنتج هذه الاسلحة شحنات عالية من الطاقة تؤدي للإضرار بالأدوات الإلكترونية وتقوض ذاكرة الحواسب، وتتميز بالدقة الشديدة في إصابة الهدف، وهناك نحو ١٢٠ دولة تقوم بتطوير طرق لاستخدام الإنترنت كسلاح لاستهداف أسواق المال ونظم الكمبيوتر الخاصة الخدمات التابعة للحكومات، وتقوم أجهزة الاستخبارات الدولية بالفعل باختبار شبكات الدول الأخرى بصورة روتينية بحثاً عن ثغرات كما ان هناك ما يشبه تشكيل قوات الكترونية [1].

ثالثا :الفضاء الالكتروني كوسيط للأعمال العدائية

يعد الإنترنت وسيطاً مفيداً بسبب التنوع والاتساع للأنشطة التي تجري من خلاله والتي تعد جزءا لا يتجزأ من طبيعة العصر الحديث والتي تتراوح أهميتها في الاقتصاد الرقمي والحكومات الالكترونية والتجارة الالكترونية فضلا عن دوره في وسائل الإعلام والاتصالات الدولية والمصارف والمنشآت الحيوية، والتي تعتمد في عملها على الإنترنت كوسيط ومن ثم فان استمراره كوسيط يعني استمرار تقديم تلك الخدمات المدنية، ومن ثم فان أي عملية هجوم قد تستهدف الإنترنت كوسيط وحامل للخدمات وناقل لها من شأنه فشل الإنترنت في القيام بوظيفته ومن ثم فان التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ إستراتيجية [2].

وتعتمد القوات المسلحة على الإنترنت في الاتصالات العسكرية بين وحدات الجيش والأجهزة الحكومية المعنية وأجهزة الاستخبارات، ويستخدم الجيش الإنترنت كمصدر للمعلومات والصورة الفضائية ويكون هناك اتصال بين الإنترنت الداخلي للجيش وبين الشبكة الدولية، ويمكن أن يتعرض الجيش للهجوم عن طريق الإنترنت بعده طرق كاختراق شبكات الجيش الداخلية وشن هجمات إنكار الخدمة للتأثير على عملية المعلومات واتخاذ القرار[3]

ويؤدي التعرض لهجوم حرمان الخدمات إلى إتلاف كم هائل من أوامر السيطرة على جهاز الكمبيوتر أو نظام ربط الشبكات على الإنترنت. ويؤدي هذا إلى شل قدرة النظام على الردّ على طلبات المستخدم، وربما يحرمه من الوصول إلى مواقع معينة على شبكة الإنترنت. وهناك عدة أشكال مختلفة لهذه الهجمات والتي يعود تاريخها على الأقل إلى الفترة التي أطلق فيها فيروس "دودة موريس" في ١٩٨٨. ويكون تاثير استخدام الفيروسات مضاعفاً نتيجة لما ينطوي عليه من توجيه "جيش" يضم مجموعة

---

(1) Arsenio T. Gumahad, **Cyber Troops and Net War: The Profession of Arms in the Information Age.** Maxwell AFB, AL: Air University, Air War College, April 1996. pp.57-156

(2) Tim Jordan," Cyber power: **The Culture and Politics of Cyberspace and the Internet"**, Rout ledge, 2000 pp 160 -254

(3) Martin C. Libicki", Conquest in Cyberspace: National Security and Information Warfare",**Op.cit** ,pp 1-14.

كبيرة من أجهزة الكمبيوتر المرتبطة بشبكة واحدة والمحملة بالفيروسات، يتم التحكم فيها عن بعد، لمهاجمة النظام المستهدف بعدد من الأوامر والطلبات في نفس الوقت ونشر الفيروسات فيه بهدف شله.

ويمكن لشخص واحد أن يتحكم بهذا "الجيش" من أجهزة الكمبيوتر. وبعض "الجيوش" التي شاركت في الهجمات على استونيا كانت تضم أكثر من مائة ألف جهاز كمبيوتر. وقد يؤدي معيار ربط شبكات الإنترنت الجديد، المعروف باسم "IPv6"، والذي كان يتوقع له أن يخفف من حدة المخاطر الأمنية، إلى زيادة نقاط الضعف في مواجهة هجمات على شاكلة هجمات الحرمان الموزع وفي خلال السنوات الماضية تمكنت فيروسات "سارس" و"لف" من الانتشار في نصف مليون جهاز كمبيوتر في اقل من أربع ساعات، وأصبحت هذه الهجمات تستخدم تعبيرا أيضا عن صراعات دولية كما استخدمت في حرب الناتو على صربيا وفي الحرب في كوسوفا وما بين التنافس بين الصين وروسيا والولايات المتحدة واستراليا وفي حرب العراق وفي الصراع العربي الإسرائيلي.[1]

رابعا: استخدام الفضاء الإلكتروني كأداة في الهجوم أو في الدفاع

تشمل العقيدة العسكرية الحالية هجمات الفضاء الالكتروني والعديد من وسائل الحرب التقليدية في إطار ما يمكن إن يطلق علية " عمليات المعلومات " (IO) والتي تعرف بأنها " الأفعال التي يمكن استخدامها للتأثير على معلومات الخصم أو أنظمة المعلومات وذلك في أثناء عملية الدفاع عن المعلومات وأنظمتها " وتشمل عمليات المعلومات عمليات الأمن،(OPSEC) والعمليات النفسية والخداع العسكري والحرب الالكترونية، والاعتداء الطبيعي التقليدي بالإضافة إلى هجمات شبكات الكمبيوتر (CNA)، وجزء من تلك الأفرع قديم قدم ظهور الحرب نفسها، ولكن تعد هجمات شبكات الكمبيوتر هي احدث وسيلة، ويتوقف نجاحها مبدئيا على الاستخبارات والقدرة على تحديد الهدف وفهم واضح لآثار ذلك الهجوم الأساسية والثانوية، حيث تصبح التقنية العالية جزءا من المهارة والخداع النفسي[2].

وقد تستخدم الدول هجمات الإرهاب الالكتروني ضد دول أخرى أو قد تستخدمها الجماعات الإرهابية، وفي السيناريو الأول قد تقوم الدوله (أ) باستخدام هجمات الفضاء الالكتروني ضد الدولة (ب) دون أن تتورط بشكل رسمي ومباشر في حرب معلنه حيث يمكنها أن في هذه الحالة في تحقيق الأهداف ذاتها التي يمكن أن تحققها الحرب التقليدية، وهناك سيناريو ثان وهو: أن تقوم الدولة (أ) باستخدام هجمات الفضاء الالكتروني كجزء من الاستعداد لنشوب صراع وحرب وهجوم تقليدي ضد الدولة (ب)، وتعد هجمات الفضاء الالكتروني اقرب إلى مفهوم "الحرب غير المتماثلة " وهو مفهوم عسكري يشير إلى الاستخدام غير المباشر للقوة وذلك بدلا من استخدام القوة بصورة مباشرة في مواجهه قوة مقابل قوة أخرى.[3]".

(1) عادل عبد الصادق " هل يمثل الارهاب الالكتروني شكلا جديدا من أشكال الصراع" ، مرجع سابق ذكره.
(2) William J. Bayles," The Ethics of Computer Network Attack", Parameters, Spring 2001, pp. 44-58.
(3) Richard A. Lipsey, "Network Warfare Operations: Unleashing the Potential", Center for Strategy and Technology, Air War College, Air University, November 2005.
, Keith B. Alexander, War fighting in Cyberspace. Joint Force Quarterly No. 46, 2007.pp58-61

وتتضمن عمليات استغلال الفضاء الالكتروني القدرة على توظيفة لخدمة وحماية نظم المعلومات ومنع تعرضة لعمليات هجومية معادية شكل يعمل على تعزيز الامن الالكترني ببعدة المتعلق بالبرمجيات والاخر بالبنية التحتية والثالث بمنع استغلالة في الحرب النفسية، وقد يستخدم الفضاء الالكتروني في عملية الهجوم بالدخول إلى شبكات الكمبيوتر والهجوم على البيانات والعمليات أو المعدات والأجهزة او شن حرب نفسية واعلامية.

أما الدفاع عن الفضاء الالكتروني فيعني القدرة على الحماية ضد هجوم أو استغلاله من الخصم "، وتأتي خطورة ذلك امكانية استخدمه من قبل الجريمة المنظمة أو القراصنة أو الإرهاب بما يؤثر على الاستقرار الاقتصادي والاجتماعي للدول التي تعتمد على الفضاء الالكتروني في البنية التحتية الكونية للمعلومات، ومن ثم يصبح من مصلحة كل الدول أن تتعاون من اجل ضمان امن وسلامة الفضاء الالكتروني حيث تصبح هناك معركة صفرية حيث يمثل المكسب لطرف خسارة للطرف الاخر وحين تستخدمها الدول كإحدى أدوات تحقيق أهدافها الإستراتيجية.[1]

## المطلب الثاني:
## هجمات الإرهاب الالكتروني
## ونمط الحرب البادرة والصراع منخفض الشدة

يمكن ان يتم تصنيف تعرض الفضاء الالكتروني لانماط الحرب والصراع الى صراع مرتفع الشدة واخر صراع منخفض الشدة، وربما يصل الى ذلك في المستقل ، بينما جاءت الحرب منخفضة الشدة بصورة مستمرة ودائمة والتي تعبرعن صراعات اعمق واكثر امد وترتبط بالصراعات ذات الطبيعه المعقدة والمتداخلة ،و أصبح الفضاء الإلكتروني ساحة لنقل الصراعات وتصفية الخلافات بكافة انواعها بين الفرقاء . ولا يمكن إحصاء الحالات التي تحتوي على هجمات إرهابيّة أو إجراميّة، ولكنّ معظمها يركز على مراكز الطاقة والبني التحتيّة ونظم الاتصالات وشركات الإنترنت ونظام مراقبة الملاحة الجويّة والمصارف ومهام الجيش وغيرها .

ويعد الصراع بكافة انماطه عبر الفضاء الإلكتروني في بدايته إلا انه سيشهد حتما في السنوات القادمة تنوعا غير مسبوق في أساليب الصراع والرقابة والدفاع وطبيعة الأطراف حين يصبح ميدان المعركة والحرب هو الفضاء الالكتروني ويرتبط بميادين الحرب الإلكترونية وباسلحة الكترونية جديدة توزات مع مثيلتها التقلدية في نتائجها التدميرية الا لم تكن قد تفوقت عليها ،و فرضت نفسها بقوة على واقع الصراعات المسلحة وغير المسلحة، وزادت التقنيات الرقمية ومدى التقدم العلمي من اضفاء درجة الفاعلية على ذلك النوع من الحروب عبر الفضاء الالكتروني ويمكن التعرض للصراع منخفض الشدة . وهي تلك الصراعات التي لا تتطور بالضرورة الى حالة استخدام القوة المسلحة، وتتميز بانها ممتدة لاتنتهي حتى بانتهاء مظاهر الصراع المسلح، وتمثل بيئة وسياق اما للتطور الى الحرب

---

[1] Ilya Kramnik," Cyberspace Wars: Militarization of Virtual Front", Moscow, News,22/05/2008

بشكلها الساحن عبر تحريك الآلة العسكرية ، او تعبر عن نمط طبيعي وخلافات تدخل في سياق التنافس الذي يعد سمة اساسية من سمات المجتمع البشري او كجزء من عمل اجهزة الاستخبارات الدولية او التنافس بين الشركات العاملة في تكنولوجيا الاتصال والمعلومات وكان ابرز مثال هو الخلاف الروسي الاستوني في مايو ٢٠٠٧ ،ويمكن التعرض على بعض انماط الصراع منخفض الشدة على النحو التالي :

اولا: - الاختراقات المتبادلة والقرصنه والطابع النوعي للصراع.

كان أول إعلان عن دخول التقنيات الرقمية ميادين الحروب في حرب البلقان في نهايات القرن الماضي على يد حلف الناتو ضد الصرب فيما سمي"بالقنابل المعتمة" ، وقد أدى هذا الهجوم الإلكتروني إلى توقف شبكة الحاسب الرئيسية مما أصاب نظم الكمبيوتر الخاصة بوزارة الدفاع اليوغسلافية بالشلل التام. واستطاعت القنابل الإلكترونية تعطيل الاتصالات عبر التشويش على شبكة الاتصالات الهاتفية الرئيسية "الثابتة" مما دفع القيادة في بلجراد إلى الاتصال بقواتها عبر الهواتف الجوالة ، وبالتالي أصبح يسيرا على قوات الحلف مهمة اختراق المكالمات. و ما تشهده الهند وباكستان من امتداد لصراعهما في الفضاء الإلكتروني عبر استخدام الفيروسات ذات الطابع القومي والتي استخدمت في تنفيذ هجمات متبادلة مضادة فيما بينهما حيث تم شن هجمات ضد أهداف تحمل مصالح وطنية وجيوبلوتيكية وفي حرب كوسوفو قامت الولايات المتحدة باستخدام النبضات الكهرومغناطيسية لإيقاف كل وسائل الاتصال اللاسلكي واللاسلكي المدنية والعسكريه، واستخدام الأقمار الصناعية في ضرب الولايات المتحدة معاقل المحاكم الإسلامية في الصومال، وكذلك في تحقيقات اغتيال رفيق الحريري رئيس وزراء لبنان الاسبق . وقد رصدت وكالة الاستخبارات الأمريكية حالة نجاح في استخدام هجمات الكمبيوتر في إصابة البنية التحتية خارج الولايات المتحدة.[1] وفي عاصفة الصحراء عام ١٩٩١ قام قراصنة من هولندا باختراق مواقع الجيش الأمريكي ونظم الإمداد والحصول على المعلومات عن مواقع الجيش الأمريكي وأسلحته وحركة السفن الحربية ، وقد كانت حرب عاصفة الصحراء ١٩٩١ في الخليج طورا انتقاليا بين حروب الثورة الصناعية وحروب المعلومات؛ فقد تواجد ما يزيد على ٣٠٠٠ حاسب متصل بحاسبات أخرى في الولايات المتحدة بينما وصفها البعض بأنها حرب مزدوجة الأساليب؛ وتمكن الاستخبارات المركزية الأمريكية من اختراق الشبكة اللاسلكية للجيش العراقي.

وفي عام ١٩٩٧ أعلنت وكالة الأمن القومي الأمريكي إن هناك خصماً ما قد تمكن من اختراق المواقع العسكرية عن طريق اختراق عمليات ونظم الكمبيوتر وفي عام ١٩٩٨ تمكن احد المخترقين من الدخول لنظم المعلومات العسكرية في إثناء الضربات العسكرية للعراق، ولكن رصد أول هجوم منظم عن طريق الإنترنت من قبل دولة ضد دولة أخرى حدث عندما استخدمته اندونيسيا في يناير ١٩٩٩ ضد نطاقات الدولة الافتراضية لتيمور الشرقية والتي كانت مدعومة بأجهزة كمبيوتر غير حكومية في ايرلندا ، كما تم توجيه الاتهام لبورما في هجوم لفيروسات ضد الانفصاليين، وفي صيف ١٩٩٩ عندما

[1] Tom Espiner," **CIA: Cyberattack caused multiple-city**",Special to CNET News.com,January 22, 2008

أعلنت تايوان على لسان رئيسها "لي تينج هو" ، دعم استقلال الجزيرة قامت الصين بشن هجمات استهدفت المواقع الحكومية لها ، وفي يناير ٢٠٠٠ قام قراصنة من أذربيجان بمهاجمة مواقع أرمينية على الإنترنت على اثر الخلاف بينهما حول السيادة الإقليمية، كما تعرضت مواقع انترنت تنتمي إلى جماعه "فالون جونج "الروحية من قبل جيش التحرير الصيني.(1)

وقامت وكالة الأمن الإسرائيليّة "شاباك" باغتيال الفدائيّ الفلسطينيّ "يحيى عيّاش" في عام ١٩٩٦ عن طريق الهاتف المحمول،وفي عام ٢٠٠٠ ، قامت مجموعة من الإسرائيليين بالهجوم على موقع لمجموعة تابعة لـ "حزب الله" في لندن، الأمر الذي قوبل بمهاجمة العرب للموقع الرئيسيّ للحكومة الإسرائيليّة وموقع وزارة الخارجية الإسرائيلية، بالإضافة إلى مهاجمة بعض الشركات الأميركيّة التي تتعامل مع إسرائيل، مثل شركة "لوسينت تكنولوجيز" للتأثير على اقتصاد إسرائيل الذي يعتمد بشكل كبير على الإنترنت.

واستطاعت مجموعة من القراصنة في رومانيا الوصول إلى الكومبيوترات التي تقوم بالتحكم والحفاظ على أجهزة الحرارة والهواء والضغط لمحطة أبحاث في القطب المتجمّد الجنوبيّ، وتهديد حياة ٥٨ عالما، والتهديد ببيع المعلومات السريّة الموجودة على أجهزة المركز لبلد آخر، لقاء مبلغ ماليّ كبير. ولحسن الحظ، فقد تمّ إيقاف القراصنة عن إتمام أعمالهم التخريبيّة قبل حدوث الضرر.(2)

وأعلنت الإدارة الأمريكية في ٧ ديسمبر ٢٠٠٥ عن تحول مهمة القوات الجوية الأساسية إلى "الطيران والقتال في الجو والفضاء الإلكتروني" ، وجاء ذكر الفضاء الإلكتروني بشكل مستقل كتعبير عن الاعتراف باستقلالية تداخل المجالات والتفوق الالكتروني ، ويشير لدورة في فاعلية مجالات العمليات الإستراتيجية ، وإضفاء أهمية إستراتيجية للفضاء الالكتروني كغيره مثل المجال الجوي والفضاء الخارجي.(3) وفي يناير ٢٠٠٦ شهدت أجهزة الحكومة البريطانية هجوما إلكترونيا من قراصنة صينيين استخدموا فيها ثغرة أمنية أثرت هذه الهجمات الإلكترونية الخبيثة على قرارات الحكومة الأمريكية بشراء أجهزة جديدة، حيث ألغت وزارة الخارجية الصفقة المنتظرة بشراء أكثر من ١٨ ألف جهاز كمبيوتر من إنتاج شركة "لينوفو الصينية" بعدما أعلن، خبراء أمن المعلومات عن مخاوفهم من وجود ثغرات أمنية في هذه الأجهزة تتسرب منها البيانات بشكل منتظم إلى الصين، وفي ٢١ يناير ٢٠٠٦ تم إنشاء فريق عمل من القوات الجوية الأمريكية للفضاء الالكتروني، وفي سبتمبر ٢٠٠٦ تم وضع مجموعه كاملة من الاقتراحات لخلق قيادة قتالية عامة في الفضاء الإلكتروني،وقد قام عدد من

(1) William yurciik & David doss ," **Internet Attacks: a policy framework for rules of engagement** ",29th Annual Telecommunications Policy Research Conference (TPRC), MIT Press, 2001 (http://arxiv.org/ftp/cs/papers/0109/0109078.pdf)

(2) فقد قام أحد القراصنة في رومانيا والذي يُدعى "بويزن وود" Poisonwood باختراق الأجهزة الخادمة الرئيسيّة والاحتياطيّة لمركز علميّ معنيّ بقياس خواصّ الإشعاعات الكونيّة الناجمة عن نظرية "الانفجار الكبير" Big Bang، وقام بوضع صفحة خاصّة عوضا عن الصفحة الرئيسيّة للموقع، تحتوي على عبارة "أنا أحبّ ملاكي لورا" I Love My Angel Laura. ومثال آخر هو قيام موظف غاضب بإطلاق مياه التصريف في المجاري غير المكرّرة في مجرى مياه الشرب في مدينة "ماروتشي شاير" Maroochy Shire في أستراليا.

(3) Courville, Shane P. **Air Force and the Cyberspace Mission: Defending the Air Force's Computer Networks in the Future.** Maxwell Air Force Base, AL, Center for Strategy and Technology, Air War College, 2007. pp.53 67.

القراصنة الصينيين بشن هجمات إلكترونية على وزارة التجارة الأمريكية ،ولم تكن هذه هي المرة الاولي بل قاموا أيضا بشن هجمات على الحكومات الغربية. وقد دفعت عملية شن الهجمات عبر الفضاء الإلكتروني ضد استونيا في ٢٠٠٧ لاهتمام الخبراء من حلف شمال الأطلنطي والاتحاد الأوربي والولايات المتحدة وإسرائيل والسفر إلى تالين عاصمة استونيا للوقوف على مجريات تلك الواقعة وعرض المساعدة والتعليم والتدريب عن الحرب الجديدة في الفضاء الإلكتروني في عصر المعلومات الذي تميز باستخدام متزايد لشبكات الاتصالات الفضائية والأرضية في الحروب [1] وفي سبتمبر عام ٢٠٠٧ اتهمت الصين بأنها تقف وراء هجمات اختراق أجهزة الكمبيوتر الخاصة بوزارة الدفاع الأمريكية، كما اتهمت بالمسئولية عن هجمات مماثلة على ألمانيا وفرنسا وبريطانيا ونيوزيلندا، وتعلن الصين أنها تقع هي الأخرى ضحية لهجمات، وذلك لسرقه معلومات وأسرار صناعية عسكرية بما أدى لتعطل خدمات الموقع مع استمرار حرب الاختراقات بين المخابرات المركزية الأمريكية وجيش التحرير الصيني [2] .

واتهم رئيس وزراء نيوزلاندا "هيلين كلارك "في ٢٠٠٧ بأن هناك عملاء لحكومة أجنبية قاموا بشن هجمات عبر الإنترنت واتهم مدير مكتب الاستخبارات الصين بالوقوف وراء تلك الهجمات ومشيرا إلى نشاطات سابقة للصين تم الكشف عنها من قبل مكتب كندي سري. [3] وقد اعترفت وزارة الدفاع الأمريكية البنتاجون بوقوع أكثر من٣٧ ألف محاولة اختراق لبرامج ومواقع تابعة للحكومة الأمريكية، إضافة إلي٨٠ إلف هجوم علي مواقع تابعة للبنتاجون علي الإنترنت وأعترف مسئولون عسكريون أمريكيون بأن بعض الهجمات نجحت في التأثير علي القدرات العسكرية الأمريكية وتعمل الإدارة الأمريكية علي منع وقوع هجمات علي مواقع الجيش والحكومة علي الإنترنت وأجهزة الكمبيوتر التابعة لها. [4]

وذلك في إطار محاولة الدول المتقدمة اختبار دفاعاتها ضد الهجمات التي يستخدم بها الكمبيوتر كسلاح دفاعي، عن طريق اختراق أنظمة الكمبيوتر بهدف التأثير في محتواها أو سرقة معلومات أو تعطيل أدائها أو تدميرها وليعكس ذلك نوعا جديدا من حروب المستقبل وأصبحت الدول تحاول تأمين منشآتها الحيوية من خطر التعرض لها، وليمثل ذلك أجواء حرب بادرة بين القوى الصاعدة في النظام الدولي، وجاء استخدام الفضاء الالكتروني ليس فقط بهدف التلصص ولكن بهدف الاستعداد لحرب المستقبل والقيام بتدريبات على استعدادات توجيه ضربة أولى لحواسب العدو، و اختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية والبنية التحتية المعلوماتية. وذلك لتحقيق "الهيمنة الالكترونية الواسعة " بشكل أسرع في حالة نشوب صراع، وهذا إلى جانب استخدام طرق أخرى من الحرب غير المتماثلة كالهجوم على الأقمار الصناعية الخاصة بالاتصالات أو محطات البث أو كابلات الاتصالات، وخاصة أن تحقيق السيطرة على الشبكات تمكن من السيطرة على الأسرار

---

(1) Robert Vamosi, **Cyber attack in Estonia--what it really means**, Special to CNET News.com, May 29, 2007
(2) **China 'hacked' into Pentagon defense system**, The Financial Times, September 4 2007
(3) Liam Tung, **China accused of cyberattacks on New Zealand,"** Special to CNET News.com, September 13, 2007
(4) China 'hacked' into Pentagon defense system, The Financial Times,op.cit

العسكرية والعلمية بما يقود إلى أن تصبح حروب المستقبل باهظة التكاليف، ومن ثم نشب الصراع من أجل تطوير القدرات في مجال أسلحة الفضاء الإلكتروني.[1] وقد أثبتت حوادث الاعتداء التي قامت بها الجماعات الإرهابية أو حتى التي اتهمت بها الدول انه مازالت هناك حالة ضعف في دفاعات الدول وأمنها المعلوماتي أمام الهجمات الالكترونية.

ثانيا: - الإرهاب الإلكتروني و رد الفعل الاحتجاجي والحرب النفسية:

يمكن استخدام الفضاء الإلكتروني في نشر الشائعات والعنصرية والكراهية الدينية إلى جانب نشر عمليات رد الفعل، كما حدث في أزمة الرسوم الكاريكاتيرية المسيئة للرسول "ص"، حيث تم تداولها وانتقالها من مجرد رسوم محلية في صحيفة محلية في الدنمرك إلى انتشارها عبر الفضاء الإلكتروني مما ساعد على قيام العديد من الاحتجاجات وتصاعد المقاومة ضد الوجود الأمريكي في أفغانستان والعراق، كما تم القيام عبر الإنترنت بحملة مضادة لتلك الرسوم من جانب المسلمون للرد على تلك الإساءات.

و كان هناك واقعه اخرى في ٢٧ مارس ٢٠٠٨ فبعدما تم رفض الحكومة الهولندية أذاعه فيلم"فتنه" Fitna المعادي للإسلام ومدته ١٥ دقيقة على المحطات التلفزيونية لجأ مخرجة النائب الهولندي المتطرف "جيرت فيلدرز" إلى عرضه على الإنترنت عبر موقع بريطاني شهير[2]. ولكن بعد الانتقادات الواسعة وردود الفعل الإسلامية و العربية والدولية الغاضبة والمنددة بعرض فيلم هولندي مسيء للإسلام تم تعليق بثه عبر الموقع وذلك بعد يوم من عرضة ولكن عرضه أثار ردود أفعال غاضبة عربيا ودوليا، فقد أدان الأمين العام للأمم المتحدة بان كي مون الفيلم بوصفه "معاديًا للإسلام". وأدان الاتحاد الأوروبي هذا العمل الذي "لا يخدم أي هدف سوى المزيد من إشعال نيران الكراهية"، و توالت ردود الأفعال المناهضة لعرض الفيلم بدعوى حرية التعبير، وادانته منظمة المؤتمر الإسلامي وجامعه الدول العربية .

وانقسمت الآراء حول الفيلم في مواقع الإنترنت والمنتديات فمنها من رآه يدخل ضمن حرية التعبير وقاموا باعادة بثه والتعبيرعن تضامنهم مع مخرج الفيلم الذي استعان أيضا خلال فيلمه بالرسوم الدنمركية المسيئة للرسول "ص" ، وعلى الجانب الأخر تباينت ردود الأفعال من جانب الدول الإسلامية بين التجاهل لها وبين التعبير عن الغضب والاستياء والتحرك دبلوماسيا تارة ثالثه حيث نجحت باكستان ومصر في استصدار قرار تاريخي من المجلس الدولي لحقوق الإنسان التابع للأمم المتحدة " يقر بان حرية التعبير لا تتضمن الإساءة للأديان والتحريض عليها أو أشاعه الآراء التي تحرض على الكراهية والتمييز" [3]. وقامت جماعه الرابطة العربية الأوروبية في هولندا بإنتاج فيلم مضاد تحت مسمى "المفتنون " عرضت فيه الاعتداء الإسرائيلي والأمريكي على الشعوب الإسلامية وتم عرض الفيلم على الإنترنت، و ظهرت امثلة عديدة كنشر صور إعدام الرئيس السابق صدام حسين عبر الإنترنت و تعرض موقع الأمم المتحدة على الإنترنت للاختراق احتجاجاً على سياسة إسرائيل والولايات المتحدة في الشرق الأوسط [4]، وتعرض

---

(1) Cyber security beware the Trojan panda, the Economist, sept. $8^{th}$-$14^{th}$ 2007 pp58.

(2) الموقع الذي تم فية اذاعه الفيلم وهو موقع بريطاني شهير هو (http://www.liveleak.com) اخر زيارة (٢- ٤- ٢٠٠٨)

(3) جريدة الأهرام ٣٠ مارس ٢٠٠٨ .

(4) جريدة الشرق الأوسط ١٩-٨-٢٠٠٧ .

موقع مسيحيي الشرق الأوسط لهجوم الكتروني من معارضين للنشاط القبطي للتنظيم من قبل "مجموعه المدافعين عن الإسلام". وقد آثارت تصريحات الشيخ القرضاوي في سبتمبر ٢٠٠٨ حول التحذير من اختراق شيعي للمجتمع السني الى حدوث هجمات وادت لاختراقات متبادلة قام بها من ينتمون إلى السنة باختراق مواقع علماء الدين الشيعة، واخترق القراصنة أكثر من ٣٠٠ موقع من المواقع الشيعية ونشروا عليها شعارات معادية للشيعة وللمذهب الشيعي، من مجموعه أطلقت على نفسها مجموعة XP بالإمارات العربية المتحدة [1]،

وقام الشيعه في ٢٩ سبتمبر ٢٠٠٨ بشن هجوم مضاد على مئات المواقع السنية طالت ٩٠٠موقع وهابي بينها مواقع لرجال دين بارزين ومن ضمنها موقع مفتي السعودية، وأعلنت مجموعة أطلقت على نفسها مجموعه الهاكرز الشيعة أنهم أقدموا علي مهاجمة المواقع السنية كخطوة انتقامية من اختراق موقع المرجع الشيعي آية الله السيستاني[2]، تبرز فيها صورة وجهٍ مصبوغ بالعلم الإيراني والآية الكريمة "فَمَنِ اعْتَدَى عَلَيْكُمْ فَاعْتَدُوا عَلَيْهِ بِمِثْلِ مَا اعْتَدَى عَلَيْكُمْ" وأصبحت هناك عملية الاستيلاء على الموقع والتحكم فيه وتدمير محتوياته وقصفها وبث رسائل معادية، كما أصبح هناك عمليات تجنيد متبادلة لتحسين القدرة على ضرب واختراق تلك المواقع على الإنترنت. وتلك الهجمات ما هي إلا انعكاسٌ لما يدور في الساحة الإسلامية من سجال بين رموز في التيارين السني والشيعي حول التبشير الطائفي وامتداد لحالة الصراع داخل المجتمعات الإسلامية. [3]

وساعد ذلك على بروز دور الفضاء الإلكتروني في التأثير السياسي والأمني والاقتصادي و استراتيجيا وفي عمل البنية التحتية الكونية للمعلومات، وكذلك كونه أصبح ساحة للصراع وللحشد والتأييد وساهمت وسائل الإعلام الالكتروني في إضافة المزيد من الزخم الإعلامي والانتشار والتأثير الواسع المدى على الرأي العام الدولي. وهناك العديد من الأمثلة التي تعبر عن استخدام الفضاء الالكتروني في الصراع ذو الطابع العرقي والطائفي والاجتماعي والاقتصادي ويتم توظيفه عن طريق استخدام الصورة والصوت والنص كوسيلة إعلام.

<u>ثالثا :- صراع وتنافس عسكري ما بين الصين والولايات المتحدة:</u>

تبنت الصين إستراتيجية حرب المعلومات كحرب للمستقبل والتي يتم خوضها لتشتيت وإثارة الاضطرابات في عملية صناعة القرارات عبر الدخول إلي أنظمة الطرف الآخر واستخدام ونقل معلوماته بعد الاهمية المتزايدة للفضاء الالكتروني.[4] وترى الصين أن من يحدد مصير المعركة ليس من يملك القوة وإنما القادر على شلّ القوة والتشويش على المعلومة. واذا كان مجال الفيروس البيولوجي كان شهد سباق في تطوير اسلحة بيولوجية فان "الفيروس الالكتروني" قد اوجد كذلك تنافسا بين العديد من الدول على الاستحواذ علية وتطويرة في اطار اسلحة الفضاء الالكتروني، بعد ان اصبح لها دور في

---

(1) جريدة القدس العربي، ٢٩ سبتمبر ٢٠٠٨.

(2) جريدة الوطن السعودية، ٢٩ سبتمبر ٢٠٠٨.

(3) عادل عبد الصادق ،" اختراق مواقع الانترنت بين السنة والشيعه..عندما تسيطر السياسة على الدين"، <u>مجلة تطبيقات مصرية</u> ،مركز الدراسات السياسية والاستراتيجية بالاهرام، العدد ١١٢، ١٥ اكتوبر ٢٠٠٨ يمكن الاطلاع علية على الرابط التالي (http://acpss.ahram.org.eg/Ahram/2008/10/15/COMM0.HTM).

(4) حنان سليمان ،" الصين تستهدف الجيش الأمريكي الكترونيا " <u>تقرير واشنطن</u>" العدد ١٤٣، ٢٦ يناير ٢٠٠٨.

تحديد مصير أي معركة وبعد الثورة في الشئون العسكرية ايضا، تعمل الصين تعمل بكل ما اوتيت من قوة على تحقيق الانتصار في هذه المعركة. وتحمل هجمات الفضاء الإلكتروني مدلول الحرب بكل معنى الكلمة ولكنها حرب قد تمنع حروبا ضارية. وفي المقابل تنفق الولايات المتحدة الكثير لتامين موقعها على الإنترنت بما قد يؤثر على الميزانية الأمريكية، ويستعمل البنتاجون ٥ ملايين حاسوب وهذه الحواسب موصولة بعضها ببعض، وهي كلها في نظر الصين أهداف عسكرية، ويتم استخدام المعلومة كسلاحٌ يستعمله الخصم في المعركة وفي "حرب الفضاء الإلكتروني "يكلف الدفاع أكثر من الهجوم، وهو دفاع مشكوك في نجاعته لأنه لا يمكن القيام بـ "مناورات سيبيرنية" لإظهار كفاءة الدفاع. وعليه فإنّ كفاءته لا تظهر إلا في حال الهجوم، وهنا يكون الوضع حرجاً لأنه في حال تهافت قدرته على صدّ الهجمات فذلك يعني أن المعركة حسمت من أولها. والصين تنفق كثيراً على هذه المعركة، ويتم تدريس "الحرب عبر الفضاء الالكتروني " كمادة في كليات الصين العسكرية."[1]

وتجمع الصين بصورة مكثفة معلومات سياسية وعسكرية وعملية من كافة أرجاء العالم لكي تسد فجواتها التكنولوجيا بأسرع ما يمكن، بالاعتماد على برامج البريد الإلكتروني أو القرصنة من مواقع على الإنترنت.، بهدف الحصول على الأسرار الصناعية والحكومية مدفوعه برغبتها في أن تصبح قوة صناعية كبرى في العالم.، ويحاول الجيش الصيني ضمان توفر المعدات والخبرات المدنية في الكمبيوتر لتساعده في تدريباته وعملياته، ويستعين بالأكاديميين ومعاهد وشركات تكنولوجيا المعلومات لدمجهم في وحدات دعم للجيش في العمليات العسكرية. وعملت الصين علي تنظيم وحدات متخصصة في الكمبيوترتصيب ملفاتها ومحتوياتها وشبكاتها.[2]

ويوجد لدى الصين جيش من "الهاكرز" القابل للتجنيد في أي وقت، بما يعد بمثابة جيش احتياطي متمرّس ومهيّأ للتدخل في أي لحظة في المعركة، ووظيفته ليس ضرب أنظمة المعلومات للبنية العسكرية الأميركية فحسب وإنما ضرب قنوات الاتصال المدنية، وعلى الرغم من عدم تكرار ما حدث في قاعدة "بيرل هاربر" الأميركية في المحيط الهادئ عسكرياً يُعد إلا أن هجمة معلوماتية على غرار "بيرل هاربر" ليست أمراً بعيد الاحتمال، كما أن تطوير الصين لقدراتها على التشويش على الاتصالات وكذلك التقدم الذي أحرزته في مهاجمه شبكات الكمبيوتر تشير إلى قدرتها على منع الجيش الأمريكي من الوصول إلى الفضاء الخارجي في إي نزاع مستقبلي ،و أهمية الأقمار الصناعية في مجال الخدمات المدنية والعسكرية، وما تشكله من أهمية قصوى للجيش الأمريكي إذ تمكنه من الحصول على سيل من المعلومات والصور والبيانات اللازمة للحرب التكنولوجية المتطورة وضمان التفوق.

وفي عام ٢٠٠٣ استطاع جيش التحرير الصيني أن ينشئ أولى وحداته الخاصة بالحرب عبر الفضاء الإلكتروني، والتي أصبحت أكثر نشاطا ضمن تنظيمات الحرب البرية ومستفيدة من الخبرات التي

---

(1) ستيفان مارشان Stephane Marchand «حين تقرر الصين أن تنتصر»، الصادر عن دار «فايار» في فرنسا،٢٠٠٧.

(2) أحد هذه الفيروسات هو فيروس "Myfip" المناسب تماما لحرب المعلومات لقدرته علي سرقة أنواع مختلفة من الملفات مثل ملفات بي دي اف و ملفات الوورد والرسومات (.dwg, .dwf) و CirCAD (.sch,.pcb) و (.dwt) وملف . ولهذا فان أي شبكة الكترونية تصاب بهذا الفيروس فإنها ستفقد وثائقها وخططها واتصالاتها وقاعدة بياناتها كما ستكون هذه المعلومات معرضة للسرقة. وخلال الأعوام الأخيرة، أجري بعض القراصنة الصينيين تجارب لاختبار الأنظمة الالكترونية الدفاعية الأمريكية على دائرة أصغر دون اللجوء إلى هجوم قوي. هذه التجارب كانت أيضا بهدف التعرف علي نقاط الضعف في الأنظمة الأمريكية ليسهل اختراقها في ما بعد.

اكتسبتها أواخر التسعينات والمتعلقة باستخدام الإنترنت وشبكات الهاتف المحمول في الرقابة والتجسس.[1] وفي السياسة الدفاعية للصين عام ٢٠٠٦ تم التأكيد على التوجه الأساسي نحو تحقيق الهدف الاستراتجي الخاص ببناء قوات مسلحة ذات صلة بالثورة المعلوماتية وتعزيز قدرتها على الانتصار في حروب المستقبل بحلول منتصف القرن ٢١[2] . وأصبح جيش تحرير الصين يرى أن عقيدته الجديدة ترتكز على أن عمليات شبكات الكمبيوتر التي هي بمثابة قوة اضافية في أي مواجهه مع الولايات المتحدة أو أي أطراف أخرى معادية أو محتملة كتايوان واليابان وكوريا الجنوبية وأيضا كندا وفرنسا وألمانيا وبريطانيا.

ويأتي اتهام الصين بشن هجمات الفضاء الالكتروني في إطار جزء من خطط بكين لفرض "هيمنة الكترونية" على خصومها العالميين بحلول عام ٢٠٥٠ في مواجهه الولايات المتحدة وبريطانيا وروسيا وكوريا الجنوبية.، وأعلنت وزاره الدفاع الأمريكية بان الجيش الصيني يعتبر الهجمات المعلوماتية "مهمة للغاية لكسب المبادرة" في المراحل الأولى من أي حرب، وان هناك قراصنة صينيون اعدوا "دليلا افتراضيا لشن حرب الكترونية وللتشويش" بعد أن درسوا كتب إرشادات وضعها حلف الأطلسي والولايات المتحدة حول الأساليب العسكرية.

وقد سجلت وزارة الدفاع الأمريكية أكثر من ٧٩ ألف محاولة قرصنة خلال عام ٢٠٠٥ نجح منها نحو ١٣٠٠ محاولة. وعلى الرغم من توجيه الاتهام إلى الصين إلا إن هذا لا يعني بالضرورة أن جيش التحرير الصيني هو قام بتلك الهجمات [3]. ويخطط البنتاجون لشن هجمات على شبكات الأعداء إذا ما قررت وكالة الأمن القومي[4]. وفي إطار محاولات للدفاع عن شبكات الكومبيوتر الحكومية تجمع وزارة الأمن الداخلي الأمريكي وتراقب معلومات عن محاولات التسلل، وتستخدم تقنيات لمنع الهجمات والعمل على خفض بوابات الحكومة على الإنترنت الى ٥٠ بوابة بعد ان كانت ٢٠٠٠بوابة لتسهيل متابعة الهجمات.[5] وهناك العديد من الأمثلة علي الهجمات الالكترونية الصينية علي الولايات المتحدة، وفي صيف عام ٢٠٠٦، أصيبت أجهزة الكمبيوتر الخاصة بمكتب الصناعة والعلوم بوزارة التجارة بأعطال جعلتها لا تتصل بشبكة الإنترنت وهو المكتب المسئول عن الصادرات التكنولوجية المتقدمة، وفي أواخر عام ٢٠٠٦، أغلقت بنوك الكمبيوتر بجامعة الدفاع القومي الأمريكي في هجوم الكتروني واسع النطاق لم يتم الإعلان عنه، و أغلقت الشبكة الالكترونية لكلية الحرب البحرية تماما بفعل هجوم صيني، وفي يونيو ٢٠٠٧، تعطلت أنظمة الاتصال (البريد الالكتروني) بمكتب وزير الدفاع دون أن يسمى البنتاجون مصدر الهجوم وان كانت تقارير إعلامية وجهت أصابع الاتهام إلي الصين. ، مما أجبر "البنتاجون" على أن يوقف عمل ١٥٠٠ كومبيوتر، ودخل المهاجمين الى البريد السريّ للوزارة، قبل

---

(1) Bill Gertz, "**China's Spies 'Very Aggressive' Threat to U.S.,**" The Washington Times, March 6, 2007, p. A3.

(2) **For an overview of China's cyber war strategies.** see James C. Mulvenon, "**Chinese Information Operations Strategies in a Taiwan Contingency.**" testimony before the U.S.–China Economic and Security Commission, September 15, 2005.

(3) جريدة الخليج ٩-٩-٢٠٠٧.

(4) "Pentagon Developing Cyberspace Weapons," Washington Technology, June 22, 1995.

(5) Ellen Nakashima," **Bush Order Expands Network Monitoring**", washingtonpost.27-1-2008

أن يتمّ إيقاف عمل أجهزة البريد الإلكتروني.(1) وفي ١٥ نوفمبر ٢٠٠٧ صدر تقرير عن الكونجرس الأمريكي يتعلق بالأمن والاقتصاد في العلاقات الصينية –الأمريكية، أشار إلى أن هناك نشاطاً صينياً موسعاً في الولايات المتحدة بما يمثل تهديداً لأمن التكنولوجيا الأمريكية (2) ،وأصبح الاختراق الالكتروني أكثر وسيلة تستخدمها الصين بفاعلية وإحدى الأدوات الهامة التي تستخدمها وكالات التجسس الصينية ضد حلفاء الولايات المتحدة أو ضد أهدف أمريكية، وفي فترة التسعينات قامت وزارة الأمن العام الصينية التي تتولى ادارة الخدمات الأمنية للدولة بعمل رائد في مجال فن السيطرة على الفضاء الإلكتروني عن طريق اختراق الشبكات الخارجية للشركات لمراقبة تدفق المعلومات عن طريق الإنترنت (3)، وتقدمت الصين بشكل كبير في مجال بناء شبكة انترنت جديدة وفي مجال التدريب والمهارة الفنية في مجال مراقبة مواقع الإنترنت وتحديد كل من مالكي المواقع والمستخدمين البالغ عددهم نحو ١٢٧ مليون بداخلها وهو ما يعزو التقدم الصيني .

وقد بلغ الانفاق العسكري على حرب الفضاء الالكتروني ١٢٧ مليون دولار من اجمالي انافق عسكري بلغ ٤٠ بليون دولار في روسيا وتحتل روسيا المركز الرابع عالميا في مجال تطوير قدرات الاسلحة الالكترونية ، بينما تاتي الصين في المركز الثاني عالميا في مجال تطوير قدرات حرب الفضاء الالكتروني وتبلغ ميزانية الانفاق عليها ٥٥ مليون دولار من انفاقها العسكري البالغ ٦٢ بليون دولار وهناك العديد من الدول التي تعكف على تطوير ترسانة الاسلحة الالكترونية . (4)

رابعا: - الإرهاب الإلكتروني وحرب الأفكار: حالة الصراع العربي الاسرائيلي

كانت حركة الأمهات الأربع الإسرائيلية قد قامت بحملة للانسحاب الإسرائيلي من جنوب لبنان لم تعبرعن نفسها كحركة سلام ولكنها ارتكزت على التكلفة العالية للحرب على أرواح الجنود الإسرائيليين وتم استغلال موقعها على الإنترنت لعرض مأساة الأمهات ممن فقدن ذويهن، وكان هناك مجموعه بريدية تم انشاؤها لمناقشة القضايا الأمنية في الشرق الأوسط.(5) وكانت البداية الحقيقية التي صعدت الهجمات "الافتراضية" cyber attacks في أكتوبر ٢٠٠٠، عندما شنت مجموعة إسرائيلية هجمات

(1) John J. Tkacik, Jr.," **Trojan Dragon: China's Cyber Threat**", The Heritage Foundation , No. 2106, February 8, 2008.
(2) **U.S.–China Economic and Security Review Commission**, 2007 Report to Congress, November 2007, p. 7.
(3) Ethan Gutmann, **Losing the New China: A Story of American Commerce, Desire and Betrayal**,San Francisco: Encounter Books, 2004, pp. 127–173
(4)Kevin G. Coleman, **The world war 111,A Cyber War has begun, Cyber Warfare, The Technolytics Institute**, September 2007(http://www.technolytics.com/Technolytics_Cyber_War.pdf)
(5) Dow Jones Newswires, **"Taiwan Military—China Cyber War More Likely Than Invasion,"** December 14, 2004;"Chinese Hacker May Be PLA," Chosun Ilbo, July 15, 2004; **"NK Hands Suspected in Cyber attacks,"** Korea Times, July 15,2004; Nautilus Institute, **"ROK Cyber attacks,"** July 15, 2004,
at (www.nautilus.org/napsnet/dr/0407/JUL1504.html#item13)
(January 28, 2008). See also Andrew Ward, **"China Blamed for Cyber Sabotage in S Korea,"** Financial Times, May 3, 2005,at http://news.ft.com/cms/s/d7ac166e-bc0a-11d9-817e-00000e2511c8.html (January 28, 2008), and CNET News, **"Flaw in Microsoft Word Used in Computer Attack,"** The New York Times, May 20, 2006, at www.nytimes.com/2006/05/20/technology/20zero.html (January 28, 2008)

على موقع حزب الله بعد أسر الجنود الإسرائيليين الثلاثة، فريق من قراصنة الإنترنت بحذف محتويات موقع حزب الله ووضع نجمة داود وعلم إسرائيل بدلا منها.ورد العرب ومؤيدوهم على الهجوم الإسرائيلي بهجمات مماثلة على مواقع حكومية إسرائيلية أهمها موقع مكتب رئيس الوزراء وموقع الكنيست وموقع غرفة التجارة وموقع بورصة إسرائيل وموقع بنك إسرائيل. وبلغ عدد المواقع التي تمت مهاجمتها نحو ٢٨٠ مقابل ٣٤ موقعا عربيا أو إسلاميا تعرضت لهجمات مماثلة وفي ٢٩ ديسمبر ٢٠٠١ تعرض ٨٠ موقعا إسرائيليا لهجمات ناجحة أدت إلى خروجها جميعا من الخدمة من ضمنها موقع رئيس الوزراء الإسرائيلي وموقع الجيش الإسرائيلي. وتعرض موقع الموساد الاسرائيلي في عام ٢٠٠٢ للاختراق وسرقة اسماء عملائة الجدد [1]

واصبحت تلك الضربات على نحو من الكر والفر ودفع ذلك إسرائيل الى تأسيس وحدة خاصة لحماية مواقع المؤسسات الحاكمة والمرافق المختلفة عام ٢٠٠٦ بعد أن تمكن قراصنة مغاربة من إتلاف ٧٥٠ موقعا إسرائيليا مرة واحدة عقب عملية "أمطار الصيف" العسكرية للجيش الإسرائيلي على غزة أبرزها المواقع الخاصة بـ"بنك إسرائيل" وحزب كاديما ومستشفى رمبام. وتركزت الجهود لاختراق أنظمة الحواسيب الكبرى بغية بناء مواقع سرية لخدمة حاجات الاتصال العملياتي وتقديم الخدمات الدعائية وتجنيد الوكلاء علاوة على سرقة عشرات آلاف رموز بطاقات الاعتماد التابعة لمواطنين في إسرائيل والولايات المتحدة . وقد تم ضرب موقع حزب الليكود في سبتمبر ٢٠٠٧ وكتب المهاجمون على صفحته بالعبرية "أنتم تقتلون الفلسطينيين ونحن نقتل حواسيبكم"، وشارك في الهجوم مجموعة خبراء فلسطينيين بعضهم من أراضي ٤٨. ودفع ذلك الى ان أسس جهاز المخابرات (الشاباك) والشرطة في إسرائيل وحدة خاصة تدعى "رام" لمواجهة حملات "الغزو الإلكتروني" التي تقودها منظمات شبابية عربية وإسلامية في العالم لتعطيل مواقع إلكترونية إسرائيلية هامة والاستحواذ خلال ذلك على رموز بطاقات الاعتماد المالية. وتعنى هذه الوحدة "رام" المشتركة للشاباك والشرطة تعنى أساسا بالدفاع عن المواقع الإستراتيجية في إسرائيل وتكشف أن ٨٥ ألف رسالة بريدية تمر عبرها كل يوم منها ١٩ ألف رسالة مفخخة. وتركز هذه المراكز في "مزرعة خاصة" تحت رعاية وزارة المالية وتخضع لرقابة وحراسة أمنية مشددة - فيزيائية وإلكترونية- وتتابع "المهاجمين" خاصة من حملة الهوية الإسرائيلية العرب.[2]

وعبرت منتديات الدردشة ومواقع الإنترنت عن الصراع العربي الإسرائيلي عبر تشكيل مجموعات مؤيدة ومتحالفة ضد جماعات أخرى بعيدا عن الأرض لتنتقل إلى الفضاء الإلكتروني، فمثلا شهد الصراع الفلسطيني -الإسرائيلي على موقع الفيسبوك حوارا حول اعتبار المستوطنين اليهود البالغ عددهم ٤٠٠ ألف في فلسطين مخالفاً للقانون الدولي مما أثار حفيظة المستوطنين وقاموا بتشكيل مجموعه على الفيسبوك بلغت ١٧٠٠ عضوا تنادي بإيقاف التمييز معبرا عن الضفة الغربية وغزة بأسماء عبرية، وقامت مجموعه تطلق على نفسها "أنها ليست فلسطين أنها إسرائيل " بلغ عدد أعضائها ما يزيد

---

(1) اختراق موقع «الموساد» في الإنترنت وكشف عملائه الجدد، جريدة الشرق الاوسط، ١٤ سبتمبر ٢٠٠٢ .

(2) وديع عواودة ،" الجهاد الإلكتروني العربي يثير مخاوف إسرائيل"، الجزيرة نت ، ٣٠-١١-٢٠٠٨
(http://www.aljazeera.net/NR/exeres/A5B34FD6-A61F-457B-8456-F1CC24EC5794.htm.

على ١٣٨٠٠عضوا، مما دفع الفلسطينين للرد السريع وقاموا بتشكيل مجموعات مضادة أطلق عليها " أنها ليست إسرائيل.. أنها فلسطين " بلغ أعضائها ٨٨٠٠ "(١). و أثار اختيار موقع الفيسبوك مسمي الضفة الغربية أو الأراضي المحتلة كتعبير حفيظة المستوطنين الإسرائيليين بما ادى الى ممارسة ضغوط على إدارة الموقع لتغييرها (٢) ويأتي هذا إلى جانب القدرة على استخدام الفضاء الالكتروني في حشد حملات التظاهر والاحتجاج وجمع التبرعات ونشر الوعي حول القضية، وحدوث تواصل بين الداخل والخارج.

خامسا: الخلاف بين استونيا و روسيا:

تعد استونيا من الدول المتقدمة في مجال تكنولوجيا الاتصال والمعلومات حيث شهد ذلك القطاع نموا منذ عام ٢٠٠٠ وفي عام ٢٠٠٧ اصبح لديها ٥٢٪ من السكان يمكنهم الدخول على الإنترنت واصبحت تعتمد وزارة الدفاع الاستونية على الإنترنت بنسبة ٦٠٪ ، كما ان هناك ٩٧٪ من العمليات المصرفية تتم عبر الإنترنت، وهناك العديد من الخدمات الحكومية ودفع الضرائب وغيرها (3)، والتي تعرضت للتوقف والتدمير اثرقيام استونيا بنقل تمثال من العهد السوفيتي يمثل الجندي المجهول الذي يعبرعن دور العرقية الروسية في مقاومة الغزو النازي.

وهذا مما اثار حملة من الغضب لدى الأقلية الروسية وحلفائها في موسكو، وقادت حملة الكراهية والاحتقان المتبادل بين الطرفين إلى بداية شن الهجوم في ٩ مايو ٢٠٠٧ الذي استهدف ضرب شبكات الاتصالات الاستونية ، وبلغت الأهداف التي تعرضت للهجوم بالمئات وتراوحت من مواقع حكومية إلى مواقع البنوك والصحف ومواقع الجامعات، وكشف الهجوم عن مشاركة متخصصين على درجة عالية من الحرفية وجاءت الهجمات من مصادر خاصة،

وتم شن الهجوم على الكمبيوتر والشبكات من أكثر من ٥٠ دولة والذي اخذ شكل موجات حيث يبدأ الهجوم ثم ينتهي فيعقبه هجوم أخر.(٤) وأتاح ارتباط استونيا القوي بشبكات الاتصال والمعلومات وجود مجال واسع من الأهداف اصبحت عرضة للهجوم مع قدرة المهاجمين على ضرب المؤسسات الرسمية للدولة وإصابة وإفساد المواقع الحكومية.(٥) وبشكل دعا وزير الدفاع "افيسكو" الى اعتبار ذلك حرب عالمية ثالثة ودعوة الأمم المتحدة لاتخاذ إجراءات في سبيل حماية الفضاء الإلكتروني (٦) لشن هجمات ضد أنظمة الكمبيوتر الخاصة بالدولة الاستونية ومن ضمنها مواقع حكومية ومواقع تخص الحزب الحاكم عن طريق هجمات "إنكار الخدمة " (٧) ، جراء شن ١٢٨ هجمة إلكترونيّة منظمة على البني التحتيّة المعلوماتية فيها خلال أسبوعين ،ترتب عليها حدوث عمليات شغب أدت إلى

(1) Rory McCarthy ," **Israel-Palestine dispute moves on to Facebook**", The Guardian, March 20 2008.

(2) David Shamah ," **Digital World: Israel or 'Palestine'?**" The Jerusalem Post , Mar 18, 2008,

(3) "Estonia Sees Red in Cyber attacks," IOL Technology, May 16, 2007.

(4) "Cyber Attacks Force Estonian Bank to Close Website," Agence France Presse, May 16, 2007.

(5) "Peter Finn, "**Cyber Assaults on Estonia Typify a New Battle Tactic,**" Washington Post, May 19, 2007.

(6) Jaak Aaviksoo, Estonian Minister of Defense, "**Cyber Defense—the Unnoticed Third World War,**" Address to the 24th International Workshop on Global Security, Paris, June 16, 2007.

(7) يقول "انج ارجما "المتحدث الرسمي باسم البرلمان الاستوني وهو يحمل درجة الدكتوراه في الفيزياء النووية "عندما نظرت إلى الانفجار النووي والانفجار الذي حدث في بلادنا في مايو ...لقد وجدت نفس الشيء ...مثل الإشعاع النووي الحرب الالكترونية عمياء ولا تميز.. أنها تدمر كل شيء " .

جرح ١٥٠ ومقتل شخص بعد انقطاع الخدمات الالكترونية ، الأمر الذي كان من الممكن أن يؤدي إلى كارثة في بلد تعتمد فيه ٩٧٪ من المعاملات المصرفيّة على الإنترنت، وقد طالبت هذه الهجمات أرقام هواتف الطوارئ المستخدمة لاستدعاء سيارات الإسعاف مما هدد ارواح المواطنين . وجاء الهجوم متطوراً ولمدة تجاوزت الساعة الكاملة، وأعلنت السلطات الإستونيّة أنّ الهجمات أتت من روسيا، وذلك بعد فترة قصيرة من تغييرها لمكان تمثال حربيّ روسيّ من الحرب العالميّة الثانية في العاصمة تالين، واحدثت تلك الهجمات صدى واسعاً حيث انه وللمرة الأولى واجهت "استونيا" هجوماً مباشراً مجهول المصدر استهدف مواقع الإنترنت الخاصة بالبنوك والوزارات والصحف وأجهزة الإعلام بما عمل على عزل استونيا عن العالم الخارجي، وعن استخدام الوسائل التي تمكنها من الكشف عن أنها تتعرض للهجوم، وكانت تلك الضربيات غير تمييزية،

وحدت تلك الهجمات من مساعي استونيا للدفاع عن حججها في الخارج. ومثل ذلك نقلة نوعية كبيرة في مجال استخدام شبكات الإنترنت كمجال جديد للحرب غير التقليدية بطريقة متطورة ومعقدة لم يسبق لها مثيل ، وتغيرت التكتيكات مع ظهور نقاط الضعف. وتم توجيه قنابل ذات حجم يصل إلى مئات الميجا بايتات إلى عنوان واحد، ثم لعنوان آخر، وهكذا.[1] ولم تعلن أي دولة أو جماعه المسئولية عن ذلك الهجوم ويدفع تعقد الهجوم للاعتقاد بانه على الأقل يمثل جهودا تتجاوز مهارات الأفراد أو الجريمة المنظمة ذاتها ويتطلب تعاوناً من قبل الدولة وشركة اتصالات ضخمة ونظراً لأن استونيا تُعد واحدة من أكثر الدول المتطورة في أنظمة اتصالاتها في أوروبا فقد تمكنت من اجتياز تلك الأزمة، ولكن دولاً أخرى كانت ستدفع ثمنا باهظاً اذا ما تعرضت لهجوم مشابه.

واستطاعت مجموعه من الهاكرز من استونيا الرد على هذا الهجوم عن طريق تعطيل منظومة الإنترنت في موسكو لمدة أسبوع كامل شلت فيها التعاملات على الشبكة، بعد اكتشاف المسئولين تعرضهم لعمليات تجسس تكنولوجي ودفاعي واسعة من روسيا، وقامت استونيا بشن هجوم مضاد استهدف إغلاق شبكة الإنترنت وشل عمليات الاتصال على نحو واسع لاسيما النطاق الحكومي إلى الحد الذي اعتبره البعض أول حرب الكترونية في التاريخ عبر الفضاء الالكتروني. كما تعرضت مواقع استونيا لفيضان من الطلبات الزائفة التي تزعم السؤال عن معلومات[2] ويسمى هذا بهجوم منع موزع الخدمة ويشمل في ذروته على أكثر من مليون جهاز حاسب آلي تشترك لإنشاء حركة تعادل ٥ آلاف نقرة في الثانية على بعض الأهداف، وكانت بعض الأجزاء منسقة تنسيقاً عالي التنظيم، وبشكل يعطي إيحاء أن هذا الهجوم يقف خلفه أكثر من مجموعة[3]

---

[1] Robert Vamosi," **Cyberattack in Estonia--what it really means"** , Special to CNET News.com, May 29, 2007., Ian Traynor, Russia accused of unleashing cyber war to disable Estonia, THE GUARDIAN, May 17, 2007

[2] Mark Landler and John Markoff," **In Estonia, what may be the first war in cyberspace"**, International Herald Tribune , Monday, May 28, 2007

[3] Shaun Waterman, **Who was behind Estonia's cyber attack?,** WORLD PEACE HERALD, Jun. 11, 2007. Available at: http://wpherald.com/articles/5127/1/Analysis-Who-was-behind-Estonias-cyber-attack/Crude-attack-unlikely-to-be-state-sponsored.html. Last visited: 01/28/2008.2007.

وفي ٢٣ يناير ٢٠٠٨ قامت استونيا بالقبض على أول مواطن روسي "ديمتري جالوشكفيتش " للاشتباه في تورطه في المشاركة في الهجوم على بنياتها التحتية المعلوماتية في ابريل ٢٠٠٧. وقد أدت المخاوف من التعرض لتلك الإخطار في روسيا إلى مطالبة أحد أعضاء الحكومة الروسية باستخدام الأسلحة النووية إذا ما تعرضت لمثل تلك الهجمات كما نظرت إدارتا كلينتون وبوش إلى تلك الأخطار على أنها تمثل استخداما للأسلحة الالكترونية. مما جعل العالم يواجه احتمال ممارسة الدول هذا النوع من الاعتداء ،وعكف عدد من دول العالم وخبراء التخطيط العسكري فيها على دراسة هذا الحدث للاستفادة منه في وضع خطط الحماية واطر التعاون.

## المطلب الثالث:

## هجمات الإرهاب الالكتروني: نمط الحرب الساخنة والصراع مرتفع الشدة

يعبر النمط ذو الطابع الساخن من الصراع عبر الفضاء الالكتروني الى تحولة لساحة موازية لحرب تقليدية دائرة حيث يكون الصراع تعبيرا عن حدة الصراع القائم بين الاطراف وهو قد يكون مقدمة لعمل عسكري او يكون مواكبا للعمليات العسكرية حيث تدور حربا عبر الفضاء الالكتروني عن طريق اختراق المواقع وقصفها وشن حرب نفسية وغيرها ، وتستمد ذلك الصراع سخونته من قوة اطرافة وارتباطة بعمل عسكري وخاصة اذا كانوا بدول فالهجمات على مواقع الإنترنت ليست مكلفة ولهذا فهي تستخدم في الحرب الحديثة فهى تكلف ٤ بالمائة مقارنه بالآلة العسكرية، بما يمكن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة دبابة ولا تستغرق إلا وقتا بسيطا. ويعد استخدام الحرب عبر الإنترنت ميزة عسكرية للأطراف المتحاربة ، والتهديد باستخدام أسلحة الفضاء الإلكتروني ضمن ترسانة الحرب الحديثة،وقد يستخدم الفضاء الالكتروني في الصراع بطريقة موازيه للحرب التقليدية كما حدث في حالة الحرب الجورجية الروسية في اغسطس ٢٠٠٨ .

اولا : حالة يوغسلافيا السابقة وتطور الحرب الالكترونية

في أولى هجمات حلف الأطلسي عام ١٩٩٩ على يوغسلافيا حدث أمر غريب أدى إلى توقف الاتصالات. لم ترصد قنابل أو صواريخ في الأجواء، حتى الدوي لم يكن مسموعا. إلا أن تفاصيله وضحت بعد فترة مع إعلان وزارة الدفاع الأمريكية أن سلاحا جديدا استخدم في أول أيام الحرب لخلع الرئيس سلوبودان ميلوسيفيتش،وكان الهجوم في أول الحرب على يوغسلافيا وكان السلاح جديدا وتمت تجربته للمرة الأولى في أرض معركة حقيقية. ويستهدف هذا السلاح شبكات الاتصالات ويعطلها ما يؤدي تلقائيا لتوقف شبكات الجيش[1]،

وهذا ما حصل مع الجيش اليوغوسلافي الذي تعطل نظام كومبيوتر أساسي لديه نتيجة ما أسماه الإعلام اليوغسلافي بصاعقة كهربائية دخلت شبكة الاتصالات وانتشرت في كل نقطة تتصل بها ومن

(1) Florian Bieber, Cyber war or Sideshow? The Internet and the Balkan Wars. Current History,No. 99: March 2000.pp 124-128.

ضمنها الكومبيوترات العسكرية، وأدي الهجوم لتوقّف الشبكة الرئيسية في يوغسلافيا، وتوقّف نظم الكومبيوتر الخاصة بالدفاع الجوي، التي كانت مهمتها استهداف طائرات حلف الأطلسي بالصواريخ.

وحدث استهداف لشبكة الهاتف الرئيسية بهدف دفع القيادة الصربية في بلجراد إلى الاتصال بقواتها عن طريق الخلوي حيث رصد المكالمات ومراقبتها واتاح الفرصة للتجسس من مركز أيشيلون الأمريكي للتنصت والمراقبة الموجود في أوروبا ،و كانت مراقبة الاتصالات الخلوية أسهل لأن عدد حملة الهاتف المحمول في يوغسلافيا يومها كان يقتصر على أركان النظام الحاكم ورجال الأعمال، مما يجعل عدد الهواتف المطلوب التنصت عليها محدودا وخلال العمليات العسكرية التي شنّتها قوات حلف شمال الأطلسي ضد الصرب، قصفت الطائرات الحربية الأمريكية محطات الكهرباء الصربية بقنبلة إلكترونية أدّت إلى إغراق معظم أراضي يوغسلافيا السابقة،وقد ألقتها طائرة أمريكية من طراز F117 على ٥ محطات طاقة صربية والتي انفجرت القنبلة وخرجت منها ملفات سلكية خاصة انتشرت في الجو كشبكة واسعة فوق خطوط الضغط العالي فعطلتها ،

وأدى ذلك إلى اشتعال النيران في المحطات، وتوقفت مراكز توزيع الطاقة اليوغسلافية عن العمل. وتوجد في داخل القنبلة (CBU94) عدة قنابل أخرى تنطلق من داخلها في الجو، وكل واحدة منها مزوّدة بمظلة صغيرة، ثم تخرج من هذه القنابل أيضا ملفات مصنوعة من الرصاص الكربوني هي التي تُكَوِّن الشبكة الإلكترونية عند اقترابها من الأرض بحيث تصيب محطات الطاقة الكهربائية والاتصالات التليفونية بالشلل التام ورغم أن هدف هذه القنابل الأساسي هو تعطيل نظم الاتصالات العسكرية والتشويش على وسائل الدفاع الجوي، إلا أنه يمكن استخدامها للتاثير على الحياة المدنية من خلال تعطيل محطات الطاقة الكهربائية.

وتعد الطاقة الموجّهة والمايكروويف أسلحة الطاقة الموجهة الحديثة ومنها أسلحة المايكروويف عالية القدرة (High Power Microwave Weapons) (HPM) من أهم الأسلحة الجديدة في مجال الحرب الإلكترونية ويمكن استخدام هذه الأسلحة لاختراق الأهداف عالية التحصين لتدمير وشلّ أسلحة الدفاع الجوي والرادارات وأجهزة الاتصال والكومبيوترات التي تعمل ضمن منظومة القيادة والسيطرة في الجيوش. كما يمكنها تدمير أجهزة التحكم في إنتاج وتخزين المواد الكيماوية والحيوية. وتنتج هذه الأسلحة شحنات عالية من الطاقة تسبب الضرر للأدوات الإلكترونية وذاكرة الكومبيوتر، وتتميز بالدقة الشديدة.

ثانيا :- الحرب بين حزب الله وإسرائيل.

شهدت الحرب الإسرائيلية التي شنت ضد الأراضي اللبنانية في ١٤ يوليو ٢٠٠٦ تواكباً واضحاً بين العمليات الحربية وبين استهداف أبراج الاتصالات الخاصة بشركات الاتصالات اللبنانية وتم اختراق شبكة الاتصالات المحمولة اللبنانية عبر شركة تيليكوم الايطالية حليف المصرية للاتصالات وذلك لتوجيه رسالة إسرائيلية إلى الشعب اللبناني تشبه المنشورات التي ترميها الطائرات الإسرائيلية على الأرض اللبنانية محذرة فيها المواطنين من تقديم إي مساعدة لحزب الله وداعية فيها إلى التخلص منة ومساعدة الإسرائيليين بكل الأشكال الممكنة ".

ودعا ذلك وزير الاتصالات اللبناني لمطالبة الشركتين بالا تقوم سنترالاتهما بتحويل إي مواد أو مكالمات من الأرقام التي تبدأ بالكود ٩٧٨ الإسرائيلي إلى الكود ٩٦٣ اللبناني، ولم يقتصر الأمر عند ذلك بل امتدت الحرب الإسرائيلية إلى التشويش على كابلات الإنترنت البحرية التي تربط لبنان بالعالم الخارجي وكذلك هوائيات الإنترنت مما أثر على قوة الاتصال بالشبكة، وشنت إسرائيل هجمات على المواقع الالكترونية لحزب الله ومؤسساته الإعلامية والسياسية [1].

وقام عدد من اللبنانيين وأصدقاء لهم بخوض حرب الكترونية لمواجهه العدوان الإسرائيلي على لبنان وذلك من خلال تأسيس لوبي لبناني في أنحاء العالم يتواصل أعضاؤه عبر مواقع الإنترنت ويجرون اتصالات لإيصال ما يتعرض له من تدمير وحصار وقتل مدنيين للتأثير على الرأي العام العالمي [2].

وسعت إسرائيل إلى إنشاء مواقع على الإنترنت لتجنيد العملاء ومناشدة المواطنين اللبنانيين أن يساعدهم على تحديد مواقع حزب الله. وتم استخدام كل من الإنترنت والهاتف النقال في دعم أهداف حربية وفي الحرب النفسية لكل طرف ضد الطرف الأخر حيث ظهرت حرب الخليوي بين إسرائيل وحزب الله للتأثير على معنويات شعبيهما، وتمكنت إسرائيل من اختراق موجات تلفزيون المنار التابع لحزب الله وقامت ببث صور لقتلى ادعت أنهم لحزب الله [3].

واعترف الجيش "الإسرائيلي" أن حزب الله استطاع وعلى مدار سنوات التنصت على المكالمات الهاتفية والخليوية في الجيش "الإسرائيلي. وتمكن حزب الله أيضا من اختراق شبكة الهواتف الخليوية بشكل متقن. واستطاع أيضاً اختراق الشبكة الخليوية التابعة لقسم الحملات في الجيش الإسرائيلي الذي فشل "في الحصول على معلومات عن حزب الله، إلى جانب فشل الموساد في تجنيد عملاء."[4]

وجرت حرب الكترونية لمهاجمة المواقع بين حزب الله وإسرائيل على الإنترنت وتميزت بعمليات الكر والفر والتخفي كما يحدث في الواقع [5]. وكجزء من الاستراتيجيات العسكرية الحديثة وشملت منع وحجب تلك المواقع أو استبدالها بصور دعائية أو إرسال رسالة معادية، وقد يشترك في تلك الحرب بعض من غير الملتزمين ايدولوجيا بكل طرف حيث تكفي الخبرة بأصول الفيروسات وفك الشفرات والقرصنة والتجسس على البريد الالكتروني وتحمل بعض رسائل الفيروسات أغراضاً سياسية وإجرامية.[6]

واستخدم النشطاء الإنترنت للمساهمة في المواجهة عن طريق الحرب النفسية والإعلامية وحشد التنديد بالسياسات الأمريكية والإسرائيلية وتبادل صور المجازر ودعم التظاهرات على الأرض والاحتياجات والإعلام عن مناطقها ومواعيدها وجمع التبرعات وعلى الجانب الأخر سعت إسرائيل إلى دفع الدبلوماسيين المتدربين لتعقب المواقع الالكترونية وغرف الدردشة لنشر الرسائل الداعمة لتل أبيب في أرجاء الفضاء الإلكتروني.

---

(1) جريدة العالم اليوم العدد، ٣١٥، الاثنين ٢٤ يوليو ٢٠٠٦.
(2) جريدة الشرق الأوسط – الثلاثاء ٢٥-٧-٢٠٠٦.
(3) جريدة الحياة اللندنية – ٦ أغسطس ٢٠٠٦.
(4) موقع جريدة عرب ٤٨ (http://www.arabs48.com/display.x?cid=6&sid=6&id=38483)
(5) جريدة الحياة ٢٩ -٧- ٢٠٠٦.
(6) Nathaniel Hoopes, New focus on cyber terrorism, CSmonitor, 15 August 2005, (www.CSmonotir.com.)

ثالثا :- الحرب بين روسيا وجورجيا.

قبل بداية الغزو الروسي لجورجيا في أغسطس ٢٠٠٨ توقفت شبكة الإنترنت الجورجية عن العمل، وتم الاعتداء على الموقع الإلكتروني للرئيس الجو رجي، وإيقافه عن العمل، ثم ظهرت على الموقع صورة الزعيم النازي أدولف هتلر، وفي نفس الوقت توقفت مواقع العديد من الوزارات والجهات الحكومية والبنوك، حتى أن وزارة الشؤون الخارجية الجورجية – خروجاً من أزمة انقطاع التواصل الإلكتروني - وضعت لنفسها بريداً إلكترونياً مجانياً على موقع البحث الإلكتروني جوجل Google، واستبدلت كذلك الموقع الإلكتروني الذي توقف فجأة بمدونة مجانية من جوجل أيضاً.

ولم تتوقف فقط العديد من المواقع الإلكترونية في جورجيا عن العمل، وإنما توقفت معظم شبكة الإنترنت لأنها كانت تعتمد إلى درجة كبيرة على كابلات الألياف الضوئية التي تمر عبر روسيا، والتي أنفقت عليها كل من روسيا والهند والصين عشرات البلايين من الدولارات لمد شبكات الإنترنت في معظم أنحاء آسيا وإفريقيا ليس فقط لتقديم خدمة يمكن أن تدر على تلك الدول دخلاً مالياً مرتفعاً كما يظن البعض، وهو الأهم أن تصبح تلك الدول هي المتحكمة في حركة تشغيل الإنترنت التي تعتمد بشكل رئيسي على تلك الكابلات ، والتي اصبح من يملكها او تمر من خلال ارضة يملك قوة إستراتيجية لا يمكن الاستهانة بها ولم تكن معظم هذه الهجمات تدار من قبل القيادة العسكرية الروسية كما قد يتبادر إلى الذهن، ولكن الكثير منها تم الإعداد له علنا بين المتعاطفين مع روسيا من قراصنة الإنترنت الروس أو ما يسمون بالهاكرز، فقد تنادوا منذ فترة تحت شعارات مثل "قف مع بلدك يا أخي".. أو "من أجل حماية روسيا والدفاع عنها" أو ما شابه ذلك من شعارات، واندلعت الحرب قبل أن تندلع العمليات العسكرية عبر الفضاء الالكتروني [1].

واتهمت الحكومة الجورجية روسيا بأنها قامت بتعطيل مواقعها على الإنترنت بما فيها موقع وزارة الخارجية الجورجية. وبسبب هذا العطل، بدأت الحكومة الجورجية في وضع تقارير وزارة الخارجية على موقع مدونات عام تمتلكه شركة جوجل وعلى الموقع الرسمي لرئيس بولندا، وفق ما ذكرته تقارير صحافية أوروبية وأميركية كما ان هناك تقارير تفيد بأن استونيا، التي تورطت في (معركة الكترونية وحرب مواقع انترنت) مع روسيا في شهر مايو ٢٠٠٧، قد أرسلت دعما فنيا إلى الحكومة الجورجية. وقد استمرت الهجمات بالتزامن مع تفجر الأزمة على مواقع الأخبار الجورجية، وتعرضت جورجيا لهجمات متفرقة ضد عدد من مواقعها على الإنترنت. مما أدى إلى تدمير عدد من المواقع التي يتم من خلالها الحصول على المعلومات والأنباء على الإنترنت. كما أن خدمة الإنترنت الجورجية تؤمن سوى دخول قليل إلى شبكة الأنباء الروسية، والتأثير على عمل المواقع التي يمكن من خلالها الحصول على معلومات عن تطورات الحرب. وقد قام بتلك الهجمات عدة مئات أو آلاف من أجهزة الكمبيوتر الشخصية المخصصة لأغراض عسكرية من أجل جعل الدخول إلى مواقع معينة شيئا صعبا أو مستحيلا.

---

(1) وقد وردت عبارة تعبر عن حجم الهزيمة وردت على الموقع البديل لوزارة الشؤون الخارجية الجورجية. تقول العبارة: "إن حربا إلكترونية روسية قد تم شنها على جورجيا وتسببت في إيقاف العديد من المواقع الرسمية للدولة، ومن بينها موقع وزارة الشؤون الخارجية.

وهنـاك مؤشـرات بـأن كـلا الجـانبين في الـصراع – أو المتعـاطفين مـع كـل منهمـا – متورطـون في الهجمات التي تستهدف منع الدخول إلى المواقع على الإنترنت و تم تنفيذ هجمات تستهدف الموقع الرسمي لحكومة أوسيتيا الجنوبية بالإضافة إلى هجمات ضد وكالة الأنباء الروسية. وقد تم تدمير موقع البنك الوطني الجو رجي واستبدل بصور للأشخاص الديكتاتوريين في القرن العشرين بالإضافة إلى صورة الرئيس الجو رجي ميخائيل ساكاشفيلي[1] واستهدف المهاجمون الروس المواقع الجورجية على الإنترنت التي يتم استضافتها من خلال خوادم في الولايات المتحدة وذلك بعد نقل استضافة موقع الرئيس الجو رجي لولاية جورجيا في الولايات المتحدة وذلك منعا من تعرضه للهجمات، وفرض الهجوم الروسي إمكانية إدخال الولايات المتحدة في الصراع. [2].

وابرز ذلك نقاط ضعف تعلق اهمها في أمرين، الأول أن معظم حركة الإنترنت في جورجيا كانت تمر بروسيا في طريقها خارج جورجيا، وبالتالي أمكن لروسيا التحكم في هذه الحركة وشلها بالكامل تقريبا. والأمر الثاني أن جورجيا كانت تعتمد حتى في التواصل الإلكتروني الداخلي على نقاط اتصال إنترنت Internet Exchange Points مملوكة لروسيا أيضاً.. أي أن حركة الإنترنت داخل جورجيا كانت تمر عبر نقاط اتصال روسية نظراً لأنها رخيصة التكلفة وهذا ما أثر على الأمن القومي.[3] وجاء الهجوم على جورجيا أكثر احترافا وتنسيقا وتعقيدا في طبيعته عن نظيرة الاستوني حيث كان نموذج استونيا يحركه الهواة ملتهبو العاطفة بينما جاء الثاني ليمثل هجوم محترفين أكثر خطورة وليعكس تطورا في استخدام الفضاء الإلكتروني في الصراعات الدولية .

رابعا: الحرب بين اسرائيل وغزة يناير ٢٠٠٩

لم يقف عجز حكومات العالم أمام العدوان الاسرائيلي على قطاع غزة حائلا امام وجود فرص لمناصرة المقاومة الفلسطينية بشتى الطرق والتي كان من ضمنها استخدام الفضاء الالكتروني والذي وفر من خلال خصائصة بيئة ملائمة لأستخدامه للمشاركة في شن عمليات الهجوم والقرصنة ضد ما المواقع المعادية وليس هذا فحسب بل استطاع هؤلاء الافراد أن يحشدوا مجموعات عديدة حليفة لينتقل من كونه رد فعل فردي الى عمل جماعي منظم للتأثير بشتى الطرق على إسرائيل وشن حملات الكترونية لتنظيم المظاهرات والاحتجاجات وجمع التبرعات حول العالم، وجاء ذلك الى جانب التحول من رد الفعل السلمي الى رد فعل عنيف من الاحتجاج عن طريق قيام القراصنة من مختلف الدول العربية والإسلامية ومن باقي دول العالم بمهاجمة مواقع إسرائيلية حيوية على الانترنت ، بهدف الضغط والحاق الضرر الاقتصادي والنفسي والسياسي بمصالح اسرائيل والعمل ايضا على استخدام الفضاء الالكتروني كوسيلة إعلام دولية الطابع لنقل ما تقترفه القوات الإسرائيلية من مجازر بحق الشعب الفلسطيني بهدف التأثير في الرأي العام الدولي.

---

(1) Tom Espiner," **Georgia accuses Russia of coordinated cyber attack**", cnit, news, August 11, 2008 (http://news.cnet.com/8301-1009_3-10014150-83.html?hhTest=1)
(2) Kevin Coleman," **Cyber War 2.0 – Russia v. Georgia**", defensetech.org, August 13, 2008 (http://www.defensetech.org/archives/004363.html)
(3) Ben Arnoldy," **Cyberspace: New Frontier in Conflicts**, .ABC News. August ١٧, 2008. (http://www.abcnews.go.com/print?id=5590834)

وانشأت حركة المقاومة الالكترونية "حماسنا " عام ٢٠٠٣ بهدف الترويج للمقاومة الثقافية والاعلامية بالاضافة الى اساليب المقاومة المعروفة التقليدية بالاضافة الى منتديات للجهاد الالكتروني .، وأنشأت سرايا القدس وهي الذراع المسلح لحركة الجهاد الإسلامي في فلسطين، وحدة الحرب الالكترونية والإعلامية المختصة، ليس فقط لترصد وتتابع ما تقوله إسرائيل بصورة شاملة، بل لتعمل على اختراق العديد من المواقع الالكترونية التابعة لأجهزة حساسة في الدولة العبرية، فيما تصل أحيانا إلى تدمير تلك المواقع عبر تقنيات برمجية يعترف بها الجميع[1]

واقام جهاز المخابرات الإسرائيلية العامة، "شاباك" وحدة خاصة باسم "رام" لمكافحة ما أسمته "الإرهاب" في الإنترنت وللمحافظة على مستخدمي الحاسوب الإسرائيليين. وفي مواجهة ما تدعيه من "إرهاب" إيران وحزب الله والقاعدة وقد اقرت اسرائيل بقدرتهم أكثر من أي مرّة لضرب مراكز الأعصاب الإسرائيلية". وتهدف اسرائيل لحماية شبكة مواقع الوزارات الحكومية الإسرائيلية المختلفة والتي أقيمت في العام ١٩٩٧، حيث يعبر من خلالها ٨٥ ألف رسالة إلكترونية في اليوم الواحد منها تسعة عشر ألفا محملة بفيروسات وبرامج خطيرة، وقد تصل إلى ٨٠ ألفا عند الهجمات . ومهمّة "رام" أن تحمي الموقع نفسه من ناحية، وأن تحمي المعلومات التي تدخل و تخرج .[2]

وظهرت حرب الفضاء الالكتروني والاختراق المتبادل بين اسرائيل وحلفائها وما بين غزة ومناصروها في يناير ٢٠٠٩ وامتد تلك المواجهه عبر الفضاء الالكتروني كجزء من حالة الحرب الدائرة وتعبيرا لها ، فقد استطاع متسللون الكترونيون (هاكرز) مسلمون اختراق مواقع إسرائيلية معروفة وتغيير ما يعرض فيها ليعكس مشاهدة ما يحدث من اعتداءات على مدينة غزة وسكانها. وتعرضت العديد من صفحات الإنترنت إلى هجمات انتقامية من مجموعات يعتقد أنها تعمل في لبنان والمغرب وإيران وتركيا. واستهدفت هذه المجموعات مواقع الشركات الإسرائيلية الصغيرة، ومواقع حكومية.[3]

وذلك بالتنسيق في ما بين أعضاء الـ"هاكرز" في المنتديات الخاصة، والصحف الإسرائيلية مثل صحيفة "معاريف"، و"يديعوت أحرونوت" باللغة الإنجليزية، وعرضت صورا لقتلى الفلسطينيين بعد تعرضهم لعمليات القصف الإسرائيلي، بالإضافة إلى صور لعمليات التعذيب التي تعرض لها المعتقلون العراقيون في السجون الأميركية. وتعرض موقع مصرف "ديسكونت" الإسرائيلي للاختراق ، بالإضافة إلى نجاح عناصر من حركة حماس اختراق موجة إذاعة الجيش الإسرائيلي وبث بيانات وما يمثل ذلك من تاثير نفسي وحرب اعلامية مضادة . ويقدرعدد الصفحات التي تعرضت لهجمات انتقامية بحوالي ١٠ آلاف صفحة، [4] على الرغم من وقف إطلاق النار بين طرفي الصراع إلا أن هناك نارا ستظل مشتعلة إما بالمقاومة بالكلمة أو بالفيروس والتي تعبر عن صراع ممتد ما بقى الصراع موجود على ارض الواقع.

---

(1) سرايا القدس ووحدة الحرب الالكترونية" موقع منصات على الانترنت، ١٧-٦-٢٠٠٨ للمزيد يمكن الدخول عبر الرابط التالي (-http://www.menassat.com/?q=ar/news-articles/3962)

(2) الشاباك يقيم وحدة رام الخاصة لمكافحة الارهاب الالكتروني والجهادي سوقع العرب ،نقلا عن صحيفة يديعوت احرونوت، ١٥-١١-٢٠٠٨ ويمكن الوصول لها عبر الرابط التالي (http://www.alarab.co.il/view.php?sel=00098272).

(3) هاكرز يخترقون ١٠ آلاف موقع إسرائيلي ،جريدة الشرق الأوسط ، ٤-١-٢٠٠٩ .

(4) جريدة الحياة اللندنية ، ٤-١-٢٠٠٩ .

# الفصل الرابع:

## موقف القانون الدولي من استخدام الإرهاب الالكتروني في حالة الصراع الدولي

# الفصل الرابع:

# موقف القانون الدولي من استخدام الارهاب الالكتروني

# في حالة الصراع الدولي

انه بالنظر إلى إمكانية تطبيق القانون الدولي على هجمات الفضاء الالكتروني فانه حري بنا إن نستند إلى مصادر ذلك القانون والتي يكون احد مصادرة إذا لم يتم إيجاد موقف قانوني واضح منها فانه يمكن الاستناد إلى العرف الدولي وكذلك القياس وأراء محكمة العدل الدولية بالإضافة إلى أراء الفقهاء وغيرها من المصادر التي تعمل على سد الفراغ التشريعي، وذلك من أجل ان يتم النظر إلى الفضاء الالكتروني على انه يجب إن يظل شانه شان غيرة من المجالات التي يمارس فيها الإنسان نشاطه محكوما بالقواعد العامة التي تحقق صالح المجموعة الدولية كلها ، وأصبح هناك اتفاق عام على سريان أحكام القانون الدولي على ما تمارسه الدول أو غير الدول لأي أنشطة داخل النظام الدولي باعتبار أن القانون الدولي قانون عام وعالمي التطبيق ، وتكون القواعد القانونية التي لا تطبق هي تلك القواعد الخاصة بالقانون الدولي التي تحكم مجالات معينة على وجه التحديد والتي لا يصح تطبيقها على الفضاء الالكتروني لتعارض طبيعته هذه المجالات وطبيعة وخصائص الفضاء الالكتروني المميزة . ويتم تناول ذلك من خلال أربعه مباحث الاول بطبيعة الجدل حول الموقف الدولي من هجمات الفضاء الالكتروني ، والمبحث الثاني يتناول مدى امكانية تطبيق القانون الدولي الانساني على هجمات الإرهاب الالكتروني ، واما المبحث الثالث فيتناول الارهاب الالكتروني في ضوء قانون الفضاء الخارجي وقانون البحار ، وأخيرا يتناول المبحث الرابع الفضاء الالكتروني وفق القانون الدولي لحقوق الإنسان.

# المبحث الأول:
# طبيعة الجدل القانوني
# حول الموقف من هجمات الفضاء الإلكتروني

يستعرض هذا المبحث طبيعة الجدل حول القوة الالكترونية والتي تم استخدامها ومدى ملائمة ذلك مع قواعد القانون الدولي وطبيعة الفجوة القانونية القائمة بين ما فرضه استخدام تلك القوة الجديدة وطبيعة المبادئ القانونية الحاكمة لاستخدام القوة في العلاقات الدولية، ومدى اعتبار هجمات الإرهاب الالكتروني نمط جديد من استخدام القوة في العلاقات الدولية ويتناول الباحث ذلك من خلال ثلاثة مطالب يتعلق المطلب الأول بتناول هجمات الفضاء الالكتروني والمبادئ العامة لمصادر القانون الدولي، وأما المطلب الثاني فيستعرض الفجوة بين الأطر القانونية الدولية وهجمات الفضاء الالكتروني، ويتناول المطلب الثالث:هجمات الإرهاب الالكتروني كاستخدام للقوة في العلاقات الدولية.

## المطلب الأول:
## هجمات الفضاء الإلكتروني و المبادئ العامة لمصادر القانون الدولي

أولا : حقوق وواجبات الدول في القانون الدولي

يسلم القانون الدولي بان للدول حقوقاً كما إن عليها واجبات، فتثبت الحقوق الطبيعية للدولة بحكم وجودها ذاته، وتتقرر تلك الحقوق لها عن طريق التعاقد أو العرف الدولي ويدخل ضمن الحقوق الأساسية للدول حق البقاء self-preservation ويعني أن لكل دولة الحق في أن تتصرف لنفسها على أي نحو يكفل لها بقاءها ويضمن استقرارها، ويترتب على ذلك انه يكون من حقها أن تأخذ ما تراه مناسبا من الوسائل للدفاع عن نفسها ضد الأخطار الخارجية التي تهدد أمنها ومصالحها العليا، ويدخل في ذلك حقها في عقد المعاهدات والمواثيق الدفاعية مع بعض القوى والأطراف الخارجية للحصول على الدعم.[1]

ويكون من حق الدولة أيضا الدخول في عضوية المنظمات الدولية والإقليمية متى كان في انضمامها إليها دعم لمقدراتها على البقاء، ويرتبط بممارسة هذا الحق حق الدفاع الشرعي عندما تكون عرضة للعدوان الخارجي عليها، وقد أكد ميثاق الأمم المتحدة هذا الحق للدولة سواء عبر ممارسة فردية أو جماعية، ويضاف إلى ذلك حق الدولة في الاستقلال Independence وهو حق ثابت للدولة بحكم ما تتمتع به من صلاحيات السيادة التي تعني انفراد الدولة دون وصاية خارجية عليها بممارسة كافة مظاهر هذه السيادة داخليا وخارجيا، وتتقيد تلك السيادة بالالتزام بقواعد القانون الدولي.

بالإضافة إلى حق المساواة Equality وان تتمتع الدول بالمساواة الكاملة القانونية مع غيرها من الدول وفقا لما تقرره قواعد القانون الدولي العام وذلك بصرف النظر عن مساحتها أو تعداد سكانها أو حجم ثرواتها، وأكد ميثاق الأمم المتحدة هذا الحق في مادته الثانية التي نصت على التزام المنظمة العالمية بكفالة مبدأ المساواة في السيادة بين جميع أعضائها، ويترتب على ذلك ألا يصبح من حق الدولة أن

---

(1) د. إسماعيل صبري مقلد " أصول العلاقات الدولية إطار علم" ، دار النهضة العربية ، الطبعة الأولى، القاهرة ، ٢٠٠٧ ,ص ص ٦-٢٠

تفرض إرادتها على أي دولة أخرى تامة السيادة في أي شأن من شئونها التي تخصها وحدها، كما يكون لكل دولة صوت واحد عند التصويت. وهناك واجب الامتناع عن التدخل في شئون الدول الأخرى نظرا لما يمثله هذا التدخل من عدوان على سيادتها أو إهدار لاستقلالها لكون هذا التدخل قد يكون مشروعا ومبررا في حالات معينة، وذلك عندما تستند الدولة المتدخلة إلى معاهدة تخولها ذلك أو عندما تطلب منها احدي الدول التدخل إلى جانبها ضد دولة أخرى معتدية، واجب تعهد الدولة بحل المنازعات الدولية التي تكون طرفا فيها بالطرق الوسائل السلمية وقد أكد ميثاق الأمم المتحدة على أهمية هذا الالتزام بنصوص صريحة وقوية لما في ذلك من حماية للسلم والأمن الدوليين.

وهناك واجب الدولة في التعاون مع الأمم المتحدة في مجال تنفيذ نظام الأمن الجماعي الذي نص علية ميثاقها، ولهذا الواجب شقان احدهما سلبي في طبيعته ويتمثل في الامتناع عن دعم ومؤازرة الدولة المعتدية والتي تزمع الأمم المتحدة تنفيذ تلك الإجراءات والتدابير العقابية ضدها، وكذلك الامتناع عن الاعتراف بأية مكاسب إقليميه تحققها الدولة المعتدية في التزام الدولة بان تضع تحت تصرف المنظمة العالمية كل ما تطلبه منها من إمكانيات لمعاقبة العدوان إعمالا للفصل السابع من الميثاق.[1]

وهناك واجب الدولة في معاملة جميع الأشخاص الذين يخضعون لسيادتها على أساس المساواة واحترام حقوق الإنسان وحرياتهم الأساسية دون تفرقة أو تمييز، ويرتبط هذا الواجب على نحو وثيق بالمحاولات الدعوبة والمضنية التي تبذلها الأمم المتحدة لحماية حقوق الإنسان وحرياتهم الأساسية من منظور التعامل معها على أنها قضية دولية وليست داخلية تلتزم الدولة باحترامها وتتحمل المسئولية عن إساءة التعامل معها من المجتمع الدولي.

ثانيا: مصادر القانون الدولي.

يمثل الإطار القانوني للعلاقات الدولية فيما أتى به القانون الدولي من قواعد وأحكام العرف الدولي المستقرة ،والتي أصبحت ترقى مع مرور الوقت إلى مرتبة القواعد القانونية المكتوبة، ويعد القانون الدولي باعتباره مجموعة من القواعد الواجبة الإتباع في علاقات الدول بعضها البعض ، ويمكن أن تنقسم مصادر القانون الدولي إلى مصادر استدلالية ومصادر رسمية ويقصد بالمصادر الاستدلالية المبادئ العامة في السلوك الدولي ،والتي استقرت فقها وعملا والتي يلجأ إليها الباحث عند عدم وجود نص تشريعي مكتوب يحكم الظاهرة وميثاق الأمم المتحدة وقراراتها والمعاهدات والقياس والعرف الدولي أما المصادر الرسمية فهي كالوثائق والاتفاقيات الدولية التي وقعتها الدول المتعاقدة.[2]

ويتكون العرف الدولي كمصدر من مصادر التشريع من عاملين أو مصدرين الأول في كتابات إعلام الفقه والملقين التي تتضمن آراءهم ومقترحاتهم في شأن أي موضوع متعلق بالنظام العام في المجتمع الدولي وهي تعكس ما تراه الدول مشروعا أو غير مشروع من تصرفاتها، إما المصدر الثاني في تكوين العرف فيتمثل في توافر عنصر العادة أو ما جرى عليه العمل بين الدول إزاء المواقف المختلفة من سلوك الدول سواء أكان عملا أو امتناع عن عمل، ويتميز ذلك العمل بالتكرار المستمر دون انقطاع

---

(1) مرجع سابق ذكره ص ص ٢٣-٢٤.
(2) مرجع سابق ذكره· ص ص ٣٩-٤٢

بحيث يمكن القول إن أغلب الدول على اتفاق فيما بينها إزاء موقف معين.[1] وتتنوع مصادر القانون الدولي إلى مصادر أصلية وتتكون من المعاهدات الدولية، ومن الاتفاقيات الرسمية التي تعقدها الدول وتهدف إلى ترتيب آثار قانونية تتفق وقواعد القانون الدولي العام وتنقسم إلى نوعين: المعاهدات العقديةContractual Treaties وهي الاتفاقيات التي تعقد بين دولتين أو أكثر لتحقيق بعض المصالح المشتركة التي تهم الدول المنضمة إليها والموقعة عليها ويقتصر أثرها على أطرافها فقط.

وهناك المعاهدات الشارعة Legislative Treaties وهي اتفاقيات متعددة الأطراف تم إبرامها بين مجموعه من الدول ويتضمن إنشاء قواعد عامة التطبيق في العلاقات الدولية وأن تعمل على حفظ وحماية مصالح المجتمع الدولي، وهناك العرف الدولي وهو من أهم مصادر القانون الدولي ومن أكثرها تسييسا لقواعده لما له من صفة العمومية التي يمتاز بها عن المعاهدات ذات القوة الإلزامية المحصورة في نطاق الإطراف المتعاقدة، ويتميز العرف الدولي أيضا بالمرونة وهناك مصدر قانوني يتعلق بالمبادئ العامة للقانون الداخلي التي ارتضتها وأقرتها الأمم المتحضرة، والتي يمكن أن يتم تطبيقها في المجال الدولي في حالة عدم وجود تصور قانوني دولي .

وهناك مصادر احتياطية للقانون الدولي مثل اجتهادات المحاكم مثل المحاكم الدولية مثل محكمة العدل الدولية مصدرا احتياطيا للقانون الدولي ، وبالإضافة إلى دور الفقه الدولي وهي الشروح التي قدمها فقهاء القانون الدولي لقواعده المتعارف عليها وإسهاماتهم في بناء نظرياته المختلفة .

وهناك مبادئ العدل والإنصاف، وخاصة وان العدالة والتي تعنى بمجموعه المبادئ التي يوحى بها العقل وحكمة التشريع الأمر الذي يجعل من فكرة العدالة فكرة مرنة، ويعد العرف باعتباره احد مصادر القانون الدولي على قدر كبير من الأهمية لما يتميز به من قدراته المرنة على المعالجة القانونية للفضاء الالكتروني كظاهرة حديثة في المجتمع الدولي وذلك أولا: لتميزه بالمرونة اللازمة للتعامل مع ظاهرة جديدة ودائمة التغير، وثانيا عدم وجود اطر قانونية واضحة تتناول تلك الظاهرة وتوضح تكيفها القانوني، فالقوانين العرفية هي قوانين غير مكتوبة والتي تتميز بصفة الاستمرار والديمومة في تطبيقها من قبل الدول وإرغامها للالتزام بها من خلال المؤسسات الدولية كالأمم المتحدة.

وكانت قانونية العلاقة بين طرق وأسس التفاعل بين دولة ودولة أخرى باعتبار أن الدولة هي الشخص الدولي المخاطب من قبل المجتمع الدولي. وانه بالنظر لإمكانية تطبيق القانون الدولي على هجمات الفضاء الإلكتروني فانه حري بنا إن نستند إلى مصادر ذلك القانون والتي يكون احد مصادرة إذا لم يتم إيجاد موقف قانوني واضح منها فانه يمكن الاستناد إلى العرف الدولي وكذلك القياس وآراء محكمة العدل الدولية بالإضافة إلى آراء الفقهاء وغيرها من المصادر التي تعمل على سد الفراغ التشريعي، وذلك من قبيل وجود ثمة اتفاق عام على سريان أحكام القانون الدولي على ما تمارسه الدول أو غير الدول لأي أنشطة داخل النظام الدولي، وذلك باعتبار أن القانون الدولي قانون عام وعالمي التطبيق، وتكون القواعد القانونية التي لا تطبق هي تلك القواعد الخاصة بالقانون الدولي التي تحكم

[1] مرجع سابق ذكره ,ص ص ٥٠-٦٢.

مجالات معينة على وجه التحديد والتي قد لا تلاءم التطبيق على الفضاء الإلكتروني وفقا لطبيعة وخصائصه المميزة. ومن ثم فإنه يمكن الاستناد للعرف والعادة والقياس والمبادئ العامة التي أقرتها الأمم المتحدة وميثاقها والمعاهدات القائمة هذا بالإضافة إلى مصادر أخرى غير رسمية كإعلان القمة العلمية لمجتمع المعلومات ٢٠٠٣ ، بالإضافة لجهود بعض المنظمات الدولية كالاتحاد الدولي للاتصالات وغيرها ، حيث يعد القياس من المصادر الاستدلالية للقانون الدولي ووسيلة هامه في استخلاص القواعد القانونية التي تحكم استخدام الفضاء الإلكتروني حيث يتم الاسترشاد في ذلك بالمواقف المماثلة وأهمية القياس كمصدر من مصادر القانون الدولي في التعامل مع ظاهرة الإرهاب الالكتروني .

وذلك من قبيل إمكانية القياس على القواعد التي تم إقرارها في مجال التعامل مع المجال الجوي وقانون البحار وقانون الفضاء الخارجي والقواعد التي تحكم المناطق القطبية وذلك مع ضرورة الأخذ في الحسبان إن طبيعة الفضاء الإلكتروني تختلف اختلافا أساسيا عن طبيعة تلك المجالات أو الفضاءات، أو أن يتم الاستناد إلى المبادئ العامة التي أقرتها الأمم المتحدة وقراراتها. ويمكن الاستفادة من المعاهدات الثنائية أو الجماعية حيث تعد مصدرا مباشرا لإنشاء القواعد القانونية الدولي وأداه فعالة تحدد للدول المتعاقدة حقوقا وتفرض بمقتضاها بواجبات معينه في علاقاتها المتبادلة، وهي بذلك تقوم بدور التشريع الداخلي، ويعزز ذلك أن الأمم المتحدة قد أصدرت قرارا عبر جمعيتها العامة برقم ١٧٢ في ٢٠ ديسمبر ١٩٦١ نص لأول مرة على سريان أحكام القانون الدولي وميثاق الأمم المتحدة على الفضاء الخارجي.

## المطلب الثاني:

## هجمات الإرهاب الإلكتروني كاستخدام للقوة في العلاقات الدولية

أولا: محددات وشروط استخدام القوة في العلاقات الدولية.

أجاز القانون الدولي التقليدي استخدام القوة باعتبارها وسيلة مشروعه من وسائل فض المنازعات الدولية وكان دور القانون الدولي مقصوراً فقط على التنظيم القانوني للحرب وكانت القوة مظهرا من مظاهر السيادة الكاملة والتي تلجأ إليها الدولة، وكانت النتائج الوخيمة الضارة للبشرية نتيجة استخدام القوة في العلاقات الدولية دافعه إلى ضرورة الحد من استخدامها واعتبار ذلك عملا غير مشروع دوليا، وذلك ابتداء من اتفاقية لاهاي للسلام ١٩٠٧ وميثاق بريان كيلوج ١٩٢٨ ثم ميثاق الأمم المتحدة عام ١٩٤٥، الذي أكد على حظر استخدام القوة أو التهديد بها في العلاقات الدولية، و أجاز ميثاق الأمم المتحدة لكل دولة حق الدفاع عن نفسها ضد عدوان خارجي يقع عليها وفرض التزامات على الدول الأخرى لمساعده الدولة المعتدى عليها وقد حددت الجمعية العامة للأمم المتحدة مفهوم العدوان والحالات التي ينطبق عليها، والتي بموجبها يحق للدولة المعتدي عليها أن تمارس حقها في مواجهه العدوان.[1] وأوجب ميثاق الأمم المتحدة على الدول أن

---

[1] أحمد عبد الونيس علي شتا ،" الدولة العاصية: دراسة في التعارض بين مواقف الدول والتزاماتها الدولية في الأمم المتحدة مع إشارة خاصة إلى إسرائيل وجنوب أفريقيا." رسالة دكتوراه، كلية الاقتصاد والعلوم السياسية، القاهرة، ١٩٨٦،ص ص ٢٣٠- ٤٥٠ .

تحل منازعاتها بالطرق السلمية والامتناع في علاقاتهم المتبادلة عن استخدام القوة أو التهديد باستخدامها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة أو بأي طريقة أخرى تتعارض مع مقاصد الأمم المتحدة ومن هنا يتضح أن الميثاق لم يحظر اللجوء لاستخدام القوة فحسب وإنما منع التهديد بها كذلك ولم يجزها إلا في حالة الدفاع الشرعي عن النفس ووفق ضوابط معينه، وقد كان ميثاق الأمم المتحدة قد أشار إلى حظر استخدام القوة في العلاقات الدولية، فان لفظ مفهوم القوة المسلحة فقط شمل كافة أنواع القوة.

ويرى الاتجاه الأول إن لفظ القوة الواردة في ٢- ٤ من الميثاق يجب تفسيره تفسيرا ضيقا، ومن ثم فان القوة غير المسلحة لا يدخل ضمن تعريف تلك المادة لمفهوم القوة، وأن تلك الأشكال قد لا تدخل ضمن هذا الحظر ويستند هؤلاء إلى النص في ديباجة الميثاق بـ " منع استخدام القوة المسلحة إلا للإغراض العسكرية "،وكذلك النص في المادة (٤٤) "انه إذا قرر مجلس الأمن استخدام القوة فانه قبل أن يطلب من عضو غير ممثل فيه تقديم القوة المسلحة "، كما إن لفظ القوة الواردة في الميثاق لا يشمل القوة المسلحة فان ما يسمى بالعدوان الاقتصادي أو الايدولوجيا تدخل ضمن التدابير التي تمثل تهديدا للسلم والأمن الدوليين والتي تقع تحت طائلة المادة ٣٩ من الميثاق وتؤكد أن الإعمال التحضيرية للمادة ٢- ٤ من الميثاق تؤكد إن مراد واضعي الميثاق من لفظ القوة هو القوة المسلحة وحيث تم استبعاد طلب البرازيل اعتبار إجراءات الضغط الاقتصادي ضمن الاستخدام غير المشروع للقوة.

ويرى الاتجاه الثاني: إن الضغوط الاقتصادية بل وكافة الأعمال الانتقامية سواء منها ما اتخذ شكل القوة المسلحة أو غيرها من الأعمال التي لا تصل إلى هذا الحد تدخل في نطاق استعمال القوة التي جرمها الميثاق، كما أن نصوص الفصل السابع من الميثاق قد تحدثت عن وسائل الميثاق وميزت بين الوسائل التي تقضي باستعمال القوة المسلحة وتلك التي لا تقضي باستعمال القوة المسلحة وأن المادة ٢- ٤ حظرت الصور المحظورة للقوة وبينت أن تلك المواجهة ضد سلامة الأرض أو الاستقلال السياسي لأية دولة والتي لا تتفق مع مقاصد الأمم المتحدة وليست القوة المسلحة وحدها هي التي من شأنها حدوث ذلك بل إن ممارسة الضغوط الاقتصادية ضد دولة معينه قد يؤدي إلى نتائج مماثلة وبطريقة ملموسة، و أن المادة ٢- ٤ من الميثاق استعملت لفظ القوة بدلاً من لفظ العنف وذلك يفيد بان الحظر شمل القوة المسلحة وسائر وسائل أساليب القهر الأخرى.

ثانيا: هجمات الإرهاب الإلكتروني كاستخدام للقوة في العلاقات الدولية

يهدف المهاجمين باستخدام الفضاء الالكتروني ليكونوا قوة إلكترونية هامة قادرة على إنزال الأضرار النفسية والاقتصادية لخدمة أهدافهم ومناصرة حلفائهم، وعلى الرغم من وجود فجوة كبيرة بين طموحات المهاجمين وبين قدراتهم الفعلية على تحقيق هذه الطموحات ولكن هذه الفجوة في طريقها للتقلص وخاصة مع التحول من عمل فردي لعمل جماعي منظم، وحدوث تبادل للخبرات والتدريب بين القراصنة من شأنه تضييق الفجوة الموجودة بين أهداف هذه المجموعات وقدراتها الفعلية على تنفيذ الهجمات ذات الطابع الفجائي ،ويؤثر ذلك على احتياطيات الأمن والحماية التي يتهددها القدرة الهائلة على الحشد والتعبئة خاصة إذا ما تم بدافع ديني وايدولوجي وغطاء شرعي في ظل محاولات الدفاع الشرعي او أعمال الانتقام او التأييد

وظهر ذلك في عملية استخدام هجمات الفضاء الإلكتروني في الحرب بين جورجيا وروسيا في أغسطس ٢٠٠٨ وفي التوتر ما بين استونيا وروسيا في مايو ٢٠٠٧ إلى ظهور الفضاء الالكتروني على الساحة الدولية وعلى نحو مباشر وعلني في الصراع الدولي ،وكأداة ووسيلة في الصراع المسلح ، و أثار ذلك الجدل حول مدى إمكانية اعتبار تلك الهجمات عملا من إعمال الحرب ، وذلك لأن تلك الهجمات جاءت متزامنة مع العمليات العسكرية التقليدية، كما أثارت التساؤلات حول التحديات التي تفرضها هجمات الفضاء الإلكتروني خاصة ما يتعلق بوجود أسلحة الكترونية وطرق جديدة للهجوم وأهداف إستراتيجية يمكن إصابتها بسهولة، وذلك ضمن ما يعرف بعمليات المعلومات (IO) وتعكس الحالة الاستونية أيضا إن تأثير هجمات الفضاء الإلكتروني على المنشآت المدنية جاء مثل الشأن العسكري التقليدي ، وان فاعلية التعاون الدولي لمساعدة استونيا كان من احد أسباب قدرتها على صد الهجوم واستعادة قواها بسرعة وتقليل نسبة التعرض للضرر.

وتقارب هجمات الإرهاب الإلكتروني الهجمات التقليدية في النتائج ولكنها تختلف في الوسائل واستراتجيات التنفيذ حيث ينتج عن استخدامها خسائر مادية في الطرف الأخر، وشن حرب نفسية وخلق حالة من شدة التنافس في بالحصول على المعلومات، و تطوير وامتلاك واستخدام ونقل الأسلحة الالكترونية في الفضاء الإلكتروني، كما حدث تنوع في وسائل الحرب أو الصراع وكذلك في الفاعلين في هذه الحرب من جماعات إرهابية أو شركات عامله في تكنولوجيا المعلومات أو حكومات أو أفراد، وهذا ما يؤدي إلى خلق حرب مفتوحة كما يفتح الباب إلى تطوير أساليب جديدة في الحرب مستقبلا.

ويكون لهجمات الفضاء الإلكتروني دوافع متنوعة كدوافع تكنولوجيه و معلوماتية واجتماعيه وثقافية وسياسية و اقتصادية وعسكرية وغيرها،ويتم شن تلك الهجمات عن طريق إحداث الضرر أو إفساد أو إنكار الخدمة أو تدمير المعلومات الموجودة في الكمبيوتر وشبكاته أو استهداف الأجهزة والمعدات كالكمبيوتر أو الكابلات البحرية أو الشبكات والتي قد تشن ضد الصناعات أو البنية التحتية الكونية للمعلومات أو شبكة الاتصالات والمجالات السياسية للنفوذ والقوى الاقتصادية الكبرى أو يتم استهداف جميع الدول.

وقد قامت وزارة الدفاع الأمريكية في عام ١٩٩٩ باختراق شبكات الكمبيوتر الصربية لإفساد العمليات العسكرية وإحداث الخلل في البنية المدنية الأساسية، وذلك في محاولة لدعم قوات التحالف وأصبح ظهور حرب المعلومات وهجمات الإرهاب الالكتروني يدفع المخططين الحربيين وغيرهم إلى تنمية قدراتهم في استخدامها وأصبحت أسلحة الفضاء الإلكتروني لها دور في تغير طبيعة الحرب حيث بدلا من المخاطرة عن طريق القيام بقصف شبكات الطاقة والسكك الحديدة وخطوط الهاتف من قبل الطيران الحربي، أصبح بإمكان استخدام شبكات الكمبيوتر والفضاء الالكتروني في إحداث الأثر نفسه عن طريق اختراق الشبكات و التأثير على عمل الطاقة الكهربائية وإفساد خدمات الاتصال والمؤسسات المالية للدولة.

وقد عني القانون الدولي الإنساني بالتفريق بين المقاتلين وغير المقاتلين بسبب نمو عدد المقاتلين وتطور أساليب الحرب واللجوء إلى استخدام أساليب الحرب الاقتصادية، ومع إن الإسهام الحقيقي للقانون الدولي الإنساني في تحديد وتقييد التسلح وابعادة الخاصة بالبعد الجغرافي: بتقليل المساحة التي يجوز فيها نشر واستخدام أنواع معينة من الأسلحة، وكذلك البعد المادي: بتقليل وسائل الحرب بفرض نوع من القيود على

كم ونوع الأسلحة المستخدمة، وأيضا ما يتعلق بالبعد العملي: بتحديد طرق استخدام هذه الأسلحة، والبعد الغائي: بفرض قيود على اختيار الأهداف التي توجه إليها الأسلحة ولذلك نجد إن تقييد التسليح يقلل من مخاطر نشوب الحرب، وكذلك ساهم القانون الدولي الإنساني في حظر توسيع العمليات العسكرية إلى المناطق المنزوعة السلاح والأماكن غير المدافع عنها والأعيان المدنية والمناطق التي تحظى بالحماية، كما حظر استخدام الأسلحة الكيماوية والبيولوجية والحارقة وكذلك فرض قيود على بعض طرق وأساليب القتال والهجمات العشوائية. (1)

ويعد القانون الدولي الإنساني هو ما يتم تطبيقه في حالة الصراع المسلح ويتضمن نوعين من القواعد الأولى التي تحد من قدرة الأطراف على استخدام وسائل وطرق الحرب والأخرى تتعلق بتلك القواعد التي تحمي الأشخاص والممتلكات في أوقات النزاع المسلح، وعلى الرغم من إن القانون الدولي الإنساني لم يحدد طبيعة النشاط العسكري إلا إن ذلك لم يعن حرية استخدام القوة بدون قيود وقواعد فقد فرض القانون حظرا على أنواع معينة من الأسلحة بالإضافة إلى أنها تتسبب في أضرار لا مبرر لها. وقد أقرت أحد القواعد الأساسية للقانون الدولي بحق الأطراف في حالة الصراع المسلح أن يختاروا الوسائل أو طرق القتال، ولكن هذا الاختيار غير مفتوح ومحدد وفق قواعد خاصة.

و يمكن أن يتسبب استخدام أسلحه الفضاء الالكتروني في إحداث أضراراً أو إصابات لا يمكن التحكم أو السيطرة على نتائجها وضعف القدرة التمييزية لها، فإنها قد تدخل تلك الهجمات ضمن الحظر بالإضافة إلى خطورتها على البنية التحتية الكونية للمعلومات والتراث الإنساني المشترك، ويرى فريق أخر اعتبار تلك الهجمات تقع ضمن الهجوم المسلح خاصة أنها تنتج إضرار كتلك الأضرار التي يسببها الهجوم التقليدي واستخدام القوة التقليدية. (2)

ويعزز هذا الموقف إن تعبير القوة الوارد ذكره في المادة ٢(٤) لم تأت مضافة في ميثاق الأمم المتحدة بما يجعل نص المادة يتسع ليشمل كافة أنواع القوة غير الشرعية، كما إن المادة ٤١ من الميثاق أشارت إلى إن استخدام الاتصالات كعامل ضغط لا يدخل ضمن القوة المسلحة "، ومن ثم فان هناك من يرى إن ذلك يمكن إن يكون بداية لإمكانية خضوع ذلك الهجوم لقواعد القانون الدولي الإنساني خاصة وانه قد فرض قواعد لاستخدام القوة في العلاقات الدولية ووضع شروط فيما عرف بقانون الحرب، ووضع التمييز بين المدنيين والعسكريين وبين المنشآت المدنية والأخرى العسكرية، وحظر استخدام الهجمات التي تنتج إضرار لا مبرر لها وفرض الاحتياطيات إثناء الهجوم، وجاء ذلك أيضا في المادة ٥٧ من البرتوكول الإضافي الأول حيث نص على أن الهجمات الانتقامية تعد شكلا من أشكال العدوان، وفرض القانون الدولي حماية خاصة للمنشآت التي تحتوي على مواده خطرة أو التي لها أهمية خاصة كمحطات الطاقة أو السدود أو المستشفيات.

(1) Daniel M. Vadnais," **Law Of Armed Conflict And Information Warfare —How Does The Rule Regarding : Reprisals Apply To An Information Warfare Attack?"** ,The Research Department ,Air Command and Staff College, March 1997,pp 5-25.

(2) Knut Dörmann," **Computer network attack and international humanitarian law"**, The Cambridge Review of International Affairs "Internet and State Security Forum", Trinity College, Cambridge, UK,19 May 2001,

ومن ثم فان أي وسيلة من وسائل الحرب يمكن أن تتعرض للمنشآت الخاضعة للحماية وفق القانوني الدولي تعد انتهاكا للسلم والأمن الدوليين وفق ما أقرة ميثاق الأمم المتحدة، فهجمات الفضاء الإلكتروني يمكن إن يتم شنها من خلال إصابة نظم المعلومات الخاصة بالتحكم والسيطرة للمرافق الحيوية الكونية بما قد يؤدي إلى إصابتها بالضرر وربما يؤدي إلى تدميرها. وهناك رأياً أخر يرى انه إذا لم يتم اعتبار هجمات شبكات الكمبيوتر والإرهاب الالكتروني هجوما مسلحا وفق القانون الدولي فانه على الأقل يجب اعتبارها تمثل تهديدا للأمن والسلم الدوليين الذي هو من مقاصد وروح ميثاق الأمم المتحدة.

ولكي يتم تطبيق القانون الدولي على هجمات الإرهاب الإلكتروني يجب أن يتم أولا: قبول التفسيرات المتعددة التي قامت على أساس تفسير "الصراع المسلح " ومفهوم " الهجوم " بما يتناسب مع التطور في آليات الهجوم وأدواته ويتفق مع روح القانون الدولي حيث إن غياب ذلك يبقى من الصعوبة تطبيق القانون الدولي الإنساني على هجمات الفضاء الإلكتروني. ثانيا: إن هجمات الإرهاب الإلكتروني يمكن اعتبارها هجوما من منطلق إمكانية استهدافها للعديد من المنشآت المحمية أو الأشخاص، وهذا ما يؤدي إلى اتساع ما يمكن إن يطلق علية "أهداف الحرب "، وثالثا عبالنظر إلى حقيقة أن هجمات الإرهاب الإلكتروني يمكن إن تمثل وسيلة حربية بدون إحداث أضرار أو جرحى بالمقارنة بالهجمات التقليدية، ورابعا: إن هجمات شبكات الكمبيوتر والإرهاب الالكتروني تضع تحديات تتعلق بمدلولات "الهجوم " كما أنها ستختبر الفهم التقليدي لحالة المحارب وذلك بسبب الاستخدام المدني للتكنولوجيا، ومعرفة كيفية اتصالها بالعمل العسكري عن طريق الكمبيوتر، وهناك فشل في وضع حدود معينة حول مشاركة المدنيين في الأعمال العدائية، وهذا ما يضعف القانون الدولي الإنساني.

وقد قام "مايكل شميت" [1] بوضع عدد من المؤشرات حول متى يمكن اعتبار هجمات الفضاء الإلكتروني استخداما للقوة وذلك من درجات تتراوح ما بين (١- ١٠) وفي حالة تطبيق تلك المؤشرات لتصل إلى درجة ٧ فإنها تعد استخداما للقوة وهذه المؤشرات هي: قسوة الهجوم Severity إذا ما كان المدنيون معرضين للقتل أو الضرر الجسيم بالممتلكات فان ذلك العمل يعد عملا عسكريا وحتى إذا كان ضرر اقل أو مشابه انه يعد استخداماً للقوة، و توافر الآنية Immediacy حيث يتم رؤية آثار الهجوم من خلال رؤيتها في دقائق أو ثوان، كما يحدث عند انفجار قنبلة تقليدية، وإذا اخذ العمل العسكري مدة تصل إلى أسابيع أو شهور، فإنها تصبح عملا دبلوماسيا أو اقتصاديا، وأيضا أن يكون العمل العسكري مباشرا Directness حيث يكون الحدث هو نتيجة لسبب مباشر حيث تكون هناك علاقة مباشرة بين السبب والنتيجة، وكذلك أن يخضع ذلك الفعل إلى القياس والملاحظة Measurability حيث يمكن أن يتم ملاحظة الحدث وقياسه كميا كحجم الخسائر المادية التي تنجم عن هذا الاستخدام، وأن يتوافر في ذلك العمل الاختراق Invasiveness حيث يتم انتهاك الحدود الدولية والدخول غير الشرعي إلى المنشآت أو المؤسسات المحمية وان يتم افتراض شرعية العمل Presumptive حيث يكون للدول الحق في احتكار الاستخدام

[1] Michael N.Schmitt," Computer networks Attack and the use of force in International law: thoughts on a normative Framework,Op.Cit.

الشرعي للقوة، والمسئولية Responsibility \legitimacy حيث يترتب على مسئولية الدولة عن العمل العسكري التزامات قانونية.[1] وهناك العديد من الهجمات لعل اهمها .

١- الهجمات على الأهداف العسكرية

تستهدف هذه النوعية من الهجمات عادة، الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات. وهذا النوع من الهجمات نادر الحدوث عادة لعدة أسباب أولها هو أنه يتطلب معرفة عميقة بطبيعة الهدف، وطبيعة المعلومات التي يجب النفاذ إليها، وهي معرفة لا تمتلكها إلا الحكومات، إضافة إلى أن الحكومات تقوم عادة بعزل المعلومات العسكرية الحساسة عن العالم، ولا تقوم بوصل الأجهزة التي تحملها بالعالم الخارجي بأي شكل من الأشكال. ولكن يبقى الحذر واجبا من عمليات التخريب الداخلية، ومن هنا تأتي ضرورة وضع نظم موثقة للتحقق من شخصيات المستخدمين، والتحديد الدقيق لطبيعة المعلومات التي يُسمح بالنفاذ إليها. ومن السيناريوهات التي تمثل هذا النوع من الهجمات النفاذ إلى النظم العسكرية واستخدامها لتوجيه جنود العدو إلى نقطة غير آمنة قبل قصفها بالصواريخ مثلا.[٢]

٢- الهجمات على الأهداف الاقتصادية

أصبح الاعتماد على شبكات الكمبيوتر شبه مطلق في عالم المال والأعمال، مما يجعل هذه الشبكات، نظرا لطبيعتها المترابطة، وانفتاحها على العالم، هدفا مغريا للعابثين والهاكر. ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل كبير بالانطباعات السائدة والتوقعات، والتشكيك في صحة هذه المعلومات، أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة، وإضعاف الثقة في النظام الاقتصادي. ومن الأمثلة على الهجمات الاقتصادية تلك العملية التي قامت بها مجموعة من الهاكر، تُعرف باسم نادي الفوضى، في عام ١٩٩٧، حيث قام هؤلاء بإنشاء بريمج تحكم بلغة آكتف إكس مصمم للعمل عبر إنترنت ويمكنه خداع برنامج كويكن Quicken المحاسبي بحيث يقوم بتحويل الأموال من الحساب المصرفي للمستخدمين. وباستخدام هذا البريمج أصبح بإمكان هؤلاء القراصنه سرقة الأموال من أرصدة مستخدمي برنامج كوي في جميع أنحاء العالم. وهو مثال واحد فقط لطرق مهاجمة شبكات المعلومات الاقتصادية واستغلالها، وهي طرق يمكن أن يكون لها آثار مدمرة على المجتمعات.[٣]

٣- الهجمات على شبكات الطاقة الكهربية

أصبح الاعتماد على شبكات المعلومات، وخصوصا في الدول المتقدمة، من الوسائل المهمة لإدارة نظم الطاقة الكهربية. ويمكن لهجمات على مثل هذا النوع من شبكات المعلومات أن تؤدي إلى نتائج خطرة وحقيقية، وخصوصا في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية. ومن الإحصائيات التي يمكن أن تدل على فعالية ذلك الهجمات التي تم شنها على العراق خلال حرب الخليج الثانية. حيث

---

(1) د.نبيل احمد حلمي "القانون الدولي وفقا لقواعد القانون الدولي العام، دار النهضة العربية،القاهرة ، ١٩٩٩، ص ص ١٢٠-٢٠٠.

(2) صفات أمين سلامة، "أسلحة حروب المستقبل بين الخيال والواقع "، دراسات استراتيجية، مركز الأمارات للدراسات والبحوث الاستراتيجية، العدد ١١٢ ،٢٠٠٥ ،ص ص ٩-٥٩.

(3) موسوعه ويكيبيديا الحره على الانترنت (/http://arz.wikipedia.org/wiki)

تشير مصادر كلية الحرب الأمريكية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى موت ما بين ٧٠ إلى ٩٠ ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية."[1] ولذلك، فإن شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشبكات الطاقة الكهربائية تعتبر من الأهداف الأولى التي قد يستهدفها الإرهاب الإلكتروني.

ثالثا: خصائص استخدام هجمات الإرهاب الإلكتروني في الصراع الدولي:

تتميز هجمات الفضاء الالكتروني باتساع درجة تاثيرها على شتى المجالات وتتميز هجمات الفضاء الإلكتروني بعده خصائص أهمها: غموض دور الفاعلين: حيث يمثل عملية تحديده الفاعلين أو المسئولية خلف الهجوم مشكلة التحديد وذلك يرجع إلى سهولة القيام بالهجوم وتنوع مستخدمي الفضاء الإلكتروني مع انتشار تكنولوجيا الاتصال والمعلومات بين عدد اكبر من السكان في بلدان كثيرة في العالم،

وهناك تجاوزاً للحدود التقليدية للدول حيث أن تلك الهجمات لا تعير أهمية للحدود الجغرافية أو السياسية حيث يمكن للهجوم أن يأتي من أي مكان في العالم وفي أي وقت، ويتميز الهجوم عبر الفضاء الإلكتروني بالسرعة في التنفيذ ،وانخفاضاً في تكلفة وسائل وأدوات الهجوم بما يجعلها عنصر جذب لفاعلين عديدين، مع الانتشار الواسع لتكنولوجيا الاتصال والمعلومات وانخفاض تكلفة الأدوات وسرعة التدريب والتعلم من خلال برامج الكمبيوتر، كما إن الأدوات التي يمكن إن تكون متاحة في العديد من المواقع على الإنترنت، وتتميز ادوات الهجوم بأنها ذاتية الحركة ولا تحتاج إلى متابعه ولا تحتاج إلا إلى التوجيه والانطلاق نحو الهدف لتحدث أضراراً كبيرة وتشكل تلك المزايا والخصائص بروزا جديدا لأخطار جديدة للأمن الدولي.

وفي ظل استخدام هجمات الارهاب الالكتروني لا توجد حدود شرعية أو واقعية لتمنع اعتداءات الاتصالات الالكترونية ومن ثم تصبح عملية شن حرب معلوماتية متاحة للجميع ويوجد لاعبون أكثر يسارعون في الانضمام لحلبة السباق، وما يكون لذلك من انعكاس على الموقف الاستراتيجي العالمي حين تشكل العناصر غير الحربية عناصر تشكل حرب المستقبل والتي تصبح حربا غير محدودة يصعب التكهن بها مع عدم وجود إنذار مبكر، وتغيرت طبيعة المقاتلين في الحرب حيث يتم الاستفادة من زيادة من كل سبل التكنولوجيا من اجل تحقيق الهدف بأقل خسائر ممكنة، وأصبحت طبيعة وحدود دور المقاتلين غير واضحة حتى للعدو في الحرب حيث يمكن أن يكون هناك حلفاء مفترضون حتى من داخل الدولة التي توجد معها في حالة نزاع مسلح ومن الممكن أن يتم اختراق تلك الدولة بسهولة، أما حدود النزاع المكانية فإنها لا ترتبط في حالة الحرب بمكان معين فقد تتم عبر الحدود حيث تصبح لا مكان لها سوى الفضاء الالكتروني وما يرتبط به من نظم تسلح أو منشآت مدنية، حيث لا توجد مواجهه مباشرة بين الأعداء بل هناك وسيطاً يحمل تفاعلات الأطراف المتصارعة ويكون هذا الوسيط معرضاً أيضا للخطر.

والمهاجم في حالة الصراع في الفضاء الإلكتروني، مثله مثل المحارب القديم، مجهّز بتقنية رخيصة لكنها قويّة، ولا تتطلب سوى تدريبٌ بسيط على استخدامها. ويمكن لحرب المعلومات أن توسّع دائرة

---

[1] Craig A. Smith," **The World Wide Web of War**". Strategy Research Project, U.S. Army War College, 21 February 2006.

المهاجمين لتشمل عدداً غير مسبوق من المبتدئين، الذين لا يحتاجون سوى لاتصال عادي بشبكة الإنترنت. وليس هناك ما يعيق التمدد الدولي للصراع عبر الفضاء الإلكتروني، كالتكلفة والجهود التي تصاحب العمل الهجومي في أغلب الأحيان ضدّ الأهداف البعيدة. فالتقنية الهجومية الحركيّة التقليدية تعتمد على الأصول المادية الملموسة ليست غالية الثمن فقط، وإنما بطيئة نسبياً أيضاً.

ورغم أن ضرر هجمات الارهاب الالكتروني ليس مألوفاً، فإنه يمكن للمشارك في الحرب أن يوقع ضرراً سريعاً من أي مكان في العالم وحتى بدون تكلفة عملياً. ويؤدي اتساع الفضاء الالكتروني لإتاحة الفرصَ لاتساع المشاركين في الصراع الذين يتسلحون أولا بالمعرفة الكافية لشن الهجمات وكذلك المعلومات عن الصراع وتطوراته وإستراتيجية الأطراف المتنازعة بما قد يعمل على إطالة أمد الصراع بما ينعكس على آثاره وتداعياته . ويرجع الأثر الكبير لاستخدام هجمات الفضاء الإلكتروني في الصراع على المستوى الدولي وذلك نظرا لدور الفضاء الإلكتروني في الحياة اليومية، الاقتصادية والاجتماعية والسياسية.

ومن ناحية أخر ى إذا تم اعتبار هجمات الإرهاب الإلكتروني تحمل خصائص الحرب فإنها ستؤثر على الحقوق والواجبات للأطراف الدولية والتي يمكن أن تكون محايدة في موقفها من النزاع، ويصعب الفصل بين حالة الحرب وحالة السلم، وقد تكون الحرب ممتدة بطول الزمن دون الدخول في عمليات قتالية على الأرض، وذلك لأن العمليات الكمبيوترية والاختراق المتبادل للمعلومات مع الخصوم يمكن أن يتم من خلال أشخاص جالسين على مقاعدهم أمام أجهزة الكمبيوتر دون الحاجة إلى الدخول في عمليات قتالية أو إرسال قوات إلى الميدان

وضعف المسئولية القانونية الدولية حول الاتهام بشن تلك الهجمات من قبل المشاركين في الصراع بما ينفي المسئولية القانونية المباشرة لأطراف الصراع ومن ثم من الصعب معاقبة المشاركين فيها. وإنه من غير الواضح ما إذا كان مرتكبو هجوم استونيا أفراداً من " مثيري الشغب المتمرسين بالإنترنت" أو أن هناك جهة رسمية ما قد أجازت عملهم. وحتى لو تم إثبات ضلوع جهة رسمية في العملية، فإنه من غير الواضح أيضاً كيف يمكن لدولة معينة أن تردّ على هجوم معلوماتي بهجوم مماثل. وأن أي تحقيق جنائي سيعاني من مشاكل كثيرة،

وحتى لو تمكن التحقيق العدلي الرقمي من تتبع أحد أجهزة الكمبيوتر المشاركة في هجوم الحرمان الموزع، فإنه يمكن عرقلة الإجراءات القانونية لمجرد كون جهاز الكمبيوتر يقع تحت سلطة قضائية غير متعاونة. وحتى لو كان هناك تنسيق وتعاون، فربما يكون جهاز الحاسوب المستخدم تابعاً لإحدى مقاهي الإنترنت أو لأحد الأماكن العامة المجهولة. وتكون خصائص هجمات الإرهاب الالكتروني وأثارها في حالة ووضع يمكن أن يقابل تلك الهجمات التي تعامل معها القانون الدولي الإنساني، وخاصة فيما يتعلق بمجهوده في حماية المدنيين ضد الهجمات ونتائجها و تعد تلك الهجمات جزءاً من إستراتيجية الإرهاب، و إحداث ثورة عسكرية جديدة مقارنة مع اختراع البارود، وطرحت هجمات الإرهاب الالكتروني تساؤلا حول ما يمكن اعتباره (حرب " أو قوة أو عدواناً من وجهه نظر القانون الدولي، وعما إذا كان رد الفعل من جراء استخدام هجمات الكمبيوتر يمكن اعتباره كذلك مقاومة مشروعه أو دفاعاً شرعياً عن النفس، وعلى العكس من ذلك هل يمكن اعتبار هجمات الإرهاب الالكتروني جزءاً من استخدام القوة وبالتالي تخضع للشرعية

القانونية وقت السلم، فإذا ما تم اعتبار استخدام الكمبيوتر كجزء من استخدام القوة في العلاقات الدولية فانه يمكن اعتبار ذلك الاستخدام أداة غير شرعية

خامسا: أسلحة الفضاء الإلكتروني والقانون الدولي

إن"الحرب عبر الفضاء الإلكتروني" ليس لها وجود مادي ملموس على أرض الواقع، لكنها تُحاكي هذا الواقع. وبهذا، فإنها حرب بلا دماء كونها صراعاً بين الموجات والإلكترونيات والبرمجيات. ويعمل "جنودها" من خلال لوحات المفاتيح وأزرار الحواسب. وتتألف ميادين القتال فيها من الألياف الضوئية وأشباه الموصلات والفضاء الإلكتروني. وتضم ترسانة أسلحتها فيروسات الكومبيوتر والنبضات الالكترونية وإشارات الليزر، وطلقات معلوماتية مُعدّة في شكل يمكن أن تحدث تدميراً جوهرياً في بعض مظاهر البنية الأساسية للعدو."[1]

و استخدم الفضاء الالكتروني أيضا في تفعيلة القدرات القتالية في ميدان القتال، والتي تتلخص في: نظم المحاكاة، والاستطلاع، والمسح الشامل للكرة الأرضية، وشبكة إنترنت إنذاريه مبكرة ومكثفة، وشبكة إنترنت قادرة على السيطرة على العمليات القتالية وغير قابلة لاخترق المعادي. بما يجعل من الأهمية بمكان لأي دولة حديثة أن تسعى إلى إيجاد كيان عصبي كمبيوتري فذ لشبكات القيادة والسيطرة على القوات، قادر على منع الاختراق والتدخّل المعادي. وظهرت أهمية التحكم في مصادر المعلومات الصديقة والمعادية، وأن تملك القدرة على تحطيم رغبة العدو في الاستمرار في القتال عن طريق مهاجمة مراكز الفكر وصنع القرار المعادية.

وهناك مبادئ عامة اقرها القانون الدولي بشان استخدام القوة في العلاقات الدولية وان كانت القوة المقصودة هي القوة الصلبة فإننا نحاول إن نجتهد في التوفيق بين إرادة المشرع الدولي وبين ما فرضته الثورة التكنولوجية من تحديات، وخاصة تلك التي تتعلق بالنزاعات المسلحة دولية الطابع أو غير الدولية، والتي تتميز بالطبيعة العرفية العامة والآمرة التي تسري في مواجهه جميع الأطراف المتحاربة بغض النظر عن كونهم أطرافا في الاتفاقيات الدولية المتضمنة لهذه المبادئ أو ليسوا كذلك. ومن هذه المبادئ التي يمكن الاسترشاد بها مبدأ حق المتحاربين في استخدام وسائل وأساليب القتال، وما يرتبط بها من حظر استخدام الأسلحة التي تسبب آلاما مفرطة وكذلك مبدأ التمييز بين المقاتلين والمدنيين وبين الأهداف العسكرية والمنشآت المدنية والمنشآت ذات الطبيعة الخطرة."[2] وجاءت القاعدة العامة في القانون الدولي الإنساني الواردة في المادة ٣٥ من البرتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جينيف الأربع لعام ١٩٤٩ لتنص على أن " حق أطراف أي نزاع مسلح في اختيار أساليب ووسائل القتال ليس حقا "لا تقيده قيود "، والمقصود بالأساليب هو طرق القتال فان الوسائل هي الأسلحة والمعدات الموضوعة بتصرف المقاتلين أطراف النزاع.[3] وتطرق القانون الدولي الإنساني إلى معالجة استخدام الأسلحة من خلال ثلاثة مستويات وهي: المبدأ

---

[1] Kevin G. Coleman, **The world war 111,A Cyber War has begun, Cyber Warfare**, The Technolytics Institute, September 2007. (http://www.technolytics.com/Technolytics_Cyber_War.pdf)

[2] Mark Russell Shulman ,"**legal constraints on information warfare**", Occasional paper, No.7, center for strategy and technology ,air war college ,March 1999.
( www.au.af.mil/au/awc/awcgate/cst/csat7.pdf)

[3] إسماعيل عبد الرحمن "الأسس الأولية للقانون الدولي الإنساني "في القانون الدولي الإنساني دليل للتطبيق على الصعيد

العـام أي تحديـد مبـادئ عامـة كإطـار شـامل لـضبط أي ثغـرة قـد يـتم تغافلـها في أيـة اتفاقيـة حاضـرة أو مستقبلا، مثل ما عرف بشرط مـارتنز "Martens clause," والـذي ورد في ديباجة اتفـاقيتي لاهـاي ١٨٩٩ و١٩٠٧ حيث نصت المادة الأولي منة على أن "يظل المدنيون والمقـاتلون في الحـالات التي لا ينص عليهـا هـذا البرتوكـول أو أي اتفاق دولي أخر تحت حماية وسلطان مبادئ القـانون الـدولي كمـا استقر بهـا العـرف والمبـادئ الإنسانية ومـا يمليـه الـضمير العـام " أي إن الأطـراف المتحاربـة لا تـستطيع مـن حيـث المبـدأ العـام التـذرع بعـدم ورود نـص صريح يتعلق بتحـريم سـلاح معين كـي تعتبر أنـة يحق لهـا استخدامه بطريقـة تتجاوز المبادئ العامـة الإنسانية المشار إليها بالتحريم السلبي.

ويعتبر القانون أي سلاح محرم استخدامه بطبيعته إذا نتج عنه آثار عشوائية ، وأن يحدث أضراراً جسيمة وآلامـا لا مبرر لهـا، و أن يلحق بالبيئة الطبيعيـة أضـرار بالغـة واسـعة الانتشار وطويلـة الأمـد، كـذلك التحـريم الايجـابي: أي تحـريم أي سـلاح ورد تحريمـه بالاسـم في إحـدى الاتفاقيـات ذات الـصلة بالقـانون، حيـث يقـسم القـانون الأسـلحة والـذخائر إلى نـوعين يتعلـق الأول: أسـلحة محرمـة أي محظـور اسـتخدامها لكونهـا وردت تسميتها بشكل واضح في معاهدات واتفاقيات دولية أهمها تلك المتعلقـة بحظـر استخدام الأسلحة الكيماويـة والبيولوجية والجرثومية والألغام المضادة للأفـراد، و الثـاني: أسـلحة مقيـد اسـتخدامها أي مسموح باسـتخدامها ولكن ضمن شروط معينة وبشكل واضح من خلال نصوص وأحكام المعاهدات والاتفاقيات ذات الصلة [1].

والتي تكون ذات طابع دولي وتقع تحت مظلة القـانون الاتفـاقي بمعنـى أنهـا ملزمـة للأطـراف الـتي انضمت لها في حين أن القواعـد والمبـادئ ذات الطـابع العـرفي والـتي تتضمنها مـصادر القـانون الـدولي الإنساني المختلفـة ملزمـة للجميـع أمـا الأسـلحة المسموح باسـتخدامها أو الـتي لم يـرد حظرهـا صـراحة في أيـة اتفاقيـة أو إعـلان أو معاهـدة ويبقـى اسـتخدامها خاضـعا للمبـادئ العامـة، وتعـرف المـادة (٤٩) مـن البرتوكـول الإضـافي الأول الهجمات "بأنها تعني بإعمال العنف ضد الخصم سواء أكان في حالة دفاع أو هجوم".

وأقـرت المـادة ٥١ أربـع مبـادئ عامـة للتعامـل مـع المـدنيين وقـت النـزاع المسلح. ولكـن هـل تعـد هجمـات الكمبيوتر تقع خارج مدلول الهجوم لأنها لا تتضمن عنف ؟ والإجابـة بـلا، وذلك لان الهجمـات المسلحة يمكـن أن تتضمن هجمات الفضاء الإلكتروني والتي يكـون لهـا تـداعيات مدنيـة، فالقـانون الـدولي الإنساني يمكـن أن يطبـق علـى هجمـات الإرهـاب الالكترونـي إذا مـا كـانـت تلـك الهجمـات تـستهدف القتـل أو التـدمير وذلـك بخلاف كبير عن طبيعة الهجمات التقليدية، و تـأتي تلك الهجمـات في طبيعـة وطـرق مختلفـة وتـتم عـبر وسـيط مختلف لكـي تتمكـن من إصابة هجمـات الكمبيـوتر المطـارات والبنيـة التحتيـة وأنظمـة الاتـصالات بمـا يحمـل تـداعيات سياسـية واقتـصادية واجتماعيـة جسيمة تتعلق بالحيـاة المدنيـة بـصفة عامـه، وذلـك مقارنـة بالهجمـات التقليديـة بـشكل يطـرح وبوضـوح التقـدم في طـرق ووسـائل الحـرب.[2] ومـن ثـم فـان التركيـز علـى نتـائج تلـك الهجمـات الـتي يـتم تنفيـذها عـبر الفـضاء الإلكترونـي يـسهل علينـا إمكـانيـة أن تخـضع تلـك الهجمـات للقـانون

---

الوطني "، دار المستقبل العربي ،القاهرة ٢٠٠٣ ص ص ٢٠١-٢٤٠.

(1) أسامة دمج: مجلة الإنساني " ربيع ٢٠٠٦.

(2) Michael N.Schmitt," Computer networks Attack and the use of force in International law: thoughts on a normative Framework,Op.Cit.

الدولي الإنساني في مبادئه العامة وذلك إذا كانت عبارة عن جزء من الأعمال العدائية التقليدية، وكما كانت هناك أهداف كانت محل الهجوم من العمليات العدائية التقليدية فإنه أصبح يوجد أهداف أخرى معرضة للخطر عن طريق استخدام هجمات الإرهاب الالكتروني بطريقة مباشرة أو غير مباشرة. وبما أوجد ذلك تداخلا بين مفهوم العدوان ومفهوم الإرهاب. وكان يعني مفهوم العدوان بشكله التقليدي بأنه "يقع ضد سلامة الأراضي والاستقلال السياسي من الدول، وأطرافها فقط دول بينما الإرهاب هو جريمة تقع ضد سلامة الأشخاص وحقوقهم وحرياتهم الأساسية وأطرافها، ولكن أوجدت هجمات الإرهاب الالكتروني تداخلا حيث يمكن أن تستهدف الدولة الأشخاص وحرياتهم كإرهاب الدولة أو إن تتعرض لسلامتها وأمنها القومي وبنياتها الأساسية الحيوية.

وفي رأى اللجنة الدولية للصليب الأحمر على اتفاقيات جينيف ١٩٤٩ والبرتوكول الإضافي لعام ١٩٧٧ أخذت بعدا أكثر اتساعا في تناولها "مفهوم "النزاع المسلح " حيث تم تعريف النزاع المسلح بأنه "أي خلاف ينشب بين دولتين ويقود إلى تدخل القوة المسلحة " وحتى لو في حالة إنكار احد الأطراف وجود حالة الحرب "، و انه بإعادة النظر في ما يتعلق بمبدأ "النسبية " والذي يتحدث عن وقوع أخطار تصيب الحياة المدنية وجرحى مدنيين ومنشآت مدنية أو التسبب في وقوع كل ما سبق "، وحيث إن هجمات الكمبيوتر بإمكانها توسيع مدى ومجال الهجوم فان فرص استهدافه للمنشآت ذات الطابع المدني تكون اكبر، وهذا ما يجعل انه ليس من العدالة أن يتم وصف ذلك على انه يمثل ضعفاً في بنية وطبيعة هجوم الإرهاب الالكتروني بقدر ما يجب أن يتم اعتباره وببساطة تعبيراً عن عملية توسع في وسائل وطرق الحرب المستخدمة والتي تعتمد على التكنولوجيا المتقدمة. وهذا ما يعني توسيع حجم الضرر الذي يمكن أن يلحق بالسكان المدنيين، وإذا ما تم التسليم بأن هجمات الإرهاب الالكتروني تعد نوعا من أنواع الهجوم، إذا ما هي الأهداف التي يمكن أن تستهدفها تلك الهجمات والتي يمكن أن تنحصر في ثلاثة أنواع تشمل الأول منها المحاربين والأهداف العسكرية والثاني المدنيين والأهداف المدنية والثالث المنشآت التي تحظى بالحماية الخاصة أو التي تستحق الحماية. فهناك من رأي انه يمكن تطبيق القانون الدولي الإنساني على هذه الهجمات عن طريق القياس والاجتهاد في المقارنة.

وهناك من رأي إن القانون الدولي الإنساني لا يمكن أن يطبق على تلك الهجمات التي تحمل طبيعة خاصة وتحتاج إلى نموذج قانوني جديد يتعامل معها وينظم استخدامها، والتي تصنف على أنها نوع من الأعمال التي تقوم به دولة أو أكثر للإضرار برعايا دولة أخرى ولا تتوقف على عمليات القتل أو الخطف أو التدمير وإنما تمتد إلى أي فعل من شانه الإضرار بالأفراد بأي شكل كان حيث لم يعد الأمر يقتصر على التصور التقليدي للصراعات المسلحة وإنما تمتد إلى كافة الأضرار التي تترتب على هذه الأفعال وما تمثله من تهديد للأهمية الإستراتيجية للفضاء الالكتروني."(1) وبذلك يمكن اعتبار الإرهاب الالكتروني أحد أهم أشكال الصراعات التي يمكن أن تستند إلى مبادئ القانون الدولي الإنساني العام والذي لا يجب أن يقتصر فقط

(1) James R. Hosek et al., **Attracting the Best: How the Military Competes for Information Technology Personnel** (Santa Monica, CA: RAND. 2003).

على الصراعات المسلحة المحدودة أو التقليدية، ففي المادة ٤٨ من البرتوكول الإضافي لعام ١٩٧٧ والتي تعد الأساس الذي يمكن الاحتكام إلية فيما يتعلق بتوفير الحماية الدولية للمدنيين في أوقات الصراعات الدولية وهذه المادة تشمل كافة الصراعات العسكرية والتي يمكن القياس عليها في حالة هجمات الإرهاب الالكتروني الموجه بشكل مباشر حيث لا يمكن التمييز بين ما هو عسكري وما هو مدني، فوفقا للمادة ٤٩ والتي تعرف الهجوم بأنة ممارسة العنف ضد الآخرين ويمكن إن يشمل ذلك كل أنواع العنف.

## المطلب الثالث:

## الفجوة بين الأطر القانونية الدولية وهجمات الفضاء الالكتروني

أولا: اثر العولمة على القانون الدولي

ترتبط العولمة بما هو دولي أو عالمي، وتشير إلى تحول العالم لقرية كونية أو عالمية."Village Global" ويدور مفهوم "العولمة" حول الوجود العالمي أو الانتشار الكوني، حيث تترك تجلّياتها تأثيراً عميقاً على التفاعل الإنساني على الأصعدة السياسية والاقتصادية والاجتماعية والثقافية، وفي إطارها النظري تعدو لتزايد التبادل و الاعتماد المتبادل بين الدول ، وإدارة المصالح المشتركة للبشرية ولصالح البشرية، وتبدو وكأنّها أصبحت ضرورة لا غنى عنها للتعامل مع كثير من القضايا البشرية خصوصاً بعد أن اتسعت دائرة الاهتمام بحقوق الإنسان وتشابكت على المستوى الكوني، وأصبحت جزءاً من القانون الدولي.[1]

وحققت "العولمة"، اتجاهاً متعاظماً نحو تخطي الحدود الجغرافية وتجاوز القيود السياسية، والقدرة الممكنة على التقاط الثقافات وتبادل التجربة الإنسانية في المجتمعات المختلفة، وعدم الأخذ بعين الاعتبار الانتماء إلى وطن محدد أو دولة معينة، وكل ذلك بفعل التطور التكنولوجي والإعلامي والمعرفي عموماً، وما رافقه من اختصار لعوامل المسافة والزمن، وهو ما ينفي الحاجة إلى التقيد بالإجراءات الحكومية الرسمية، وهو ما يقود طبيعياً إلى إسقاط القوانين بكل ما تعنيه هذه القوانين من ضبط للأداء الإنساني في أبعاده وأنماطه الاجتماعية العامة، والتي تعطي للثقافة هويتها الخاصة، وللهوية ثقافتها الخاصة.

وللعولمة شقان أولهما شق مادي ملموس نشأ نتيجة التطور العلمي والتكنولوجي، وثورة المعلومات من خلال وسائل الاتصال والإعلام، وانتشار المحطات الفضائية التي تعم برامجها كل أرجاء الكرة الأرضية، وتصل نسبياً إلى غالبية البشر، وثانيهما: شق قيمي نشأ نتيجة التوسع التنافسي للإنتاج الرأسمالي الذي فرض اقتصاد السوق على العالم، وساعد الانتشار السريع لتكنولوجيا الاتصال والمعلومات من حركة الاعتماد المتبادل بين دول العالم على المستوى الاقتصادي وأهمية دورها في النمو الاقتصادي العالمي المتمثل في الاقتصاد الرقمي على حساب القطاعات الأخرى التقليدية في الاقتصاد، وكان لذلك تأثير على دور الدول وتأثيرها في العلاقات الدولية حيث جاءت التغيرات في البيئة الدولية

---

[1] سعيد حسين محمود غلاب، "التطورات الراهنة في النظام الدولي وأثرها على مبدأ استخدام القوه في العلاقات الدولية " رسالة دكتوراه غير منشورة، كلية الاقتصاد والعلوم السياسية، جامعه القاهرة، ٢٠٠٥ ،ص ص ٣٠٠-٣٢٧.

من جراء اعتماد الاقتصاد على المعرفة وتدفق المعلومات بدلا من الاعتماد على المواد الخام أو الموارد الطبيعة أو التجارة.

وأصبح لتكنولوجيا الاتصال والمعلومات دور في دعم التجارة الالكترونية وتقديم الخدمات الحكومية وعمل المؤسسات المالية وتقديم الخدمات الحكومية إلى أن أصبحت بمثابة عصب التقدم والحياة المعاصرة، وكان لذلك تأثيرات على سيادة الدول بعد إن اجتازت الشبكات الحدود التقليدية للدول وعملت على الانتقال الحر والسريع للمعلومات من الدول والى الخارج والعكس بدون عوائق جمركية أو سيادية، وحدث تراكم جديد للثروة وإعادة توزيع للقوة بين دول العالم وأصبحت المعرفة والمعلومات هي مصدر الثروة مع قلة الاعتماد على القوة العسكرية والموارد الطبيعة كمصادر للقوة.

وأحدثت الثورة التكنولوجية تغييرات في الشئون العسكرية حيث أثرت على المعرفة الكاملة بالذات والخصم بما يظهر في الوعي الكامل بميدان المعركة وعملت على تعقد الجهود لمسالة التفريق ما بين الأهداف العسكرية والأخرى المدنية، وهذا بالإضافة للمساعدة على إمكانية إحداث الضرر البالغ بالمدنيين والمنشآت وبما مثل خطرا على الالتزام بقانون النزاعات المسلحة [1]. أما على صعيد القانون الدولي ذاته فلم يعد قانون دول بل قانون علاقات دولية، وأصبح هناك فواعل لم ترق بعد إلى مرتبة الشخص القانوني الدولي إلا أنها اكبر مؤثر في صنع القاعدة القانونية بطريقة ما فالقانون أصبح يحكم مجمل علاقات الدول ووحداتها، وحدث للمصادر الشكلية للقانون الدولي ثمة تطور من جراء ثوره تكنولوجيا الاتصال والمعلومات، وهناك فجوة واضحة بين القواعد المنظمة للعلاقات الدولية والممارسة الفعلية لأعضاء النظام الدولي.[2]

وجاء ذلك ضمن التحديات السياسية والاقتصادية والأمنية والقانونية التي فرضتها التغييرات التكنولوجية والاتصالية أمام القانون الدولي الذي تعامل أساسا مع مفاهيم القوة الصلبة واستخداماتها واتسم بالجمود والمحافظة _منذ اتفاقية ويستفاليا ١٦٤٨ _و تراجع في حيثياته وأطره القانونية أمام تصاعد القوة اللينة والتي أفضت إلى أنشطة جديدة لم تتوافق مع تلك الأطر، أو أنها كشفت عن تناقضها مع تلك المبادئ القانونية الموجودة، أو أنها كشفت أن هناك بعض القواعد القانونية التي يمكن تطبيقها في مبادئها العامة، كما في اتفاقيات جينيف لعام ١٩٤٩ والبروتوكولات المكملة لها في عام ١٩٧٧ والقانون الدولي العرفي، وحتى إن اتفاقية جينيف ركزت على حماية الأشخاص وقت الحرب دون الإشارة إلى أسلحة محددة ولم يقدم البروتوكولان الإضافيان اشاره إلى طرق وأنواع الحرب المختلفة إلا في خصائصها العامة.

و كانت الاتفاقيات الأصلية التي وقعت عام ١٨٦٤ ثم طورت عام ١٩٤٩تعاملت مع مفهوم واحد للحرب وهى الحرب التي تخوضها الجيوش النظامية بين الدول القائمة، عاكسة بذلك طبيعة الصراع

---

(1) LTC _ryan W. Ellis," **The International Legal Implications and Limitations of Information Warfare: What Are Our Options?"**, USAWC Strategy Research Project,U.S. Army War College, 2001,

(2) د.احمد عبد الونيس "_العولمة والقانون الدولي "، د.حسن نافعة &د.سيف الدين عبد الفتاح (محرران) ، سلسلة محاضرات الموسم الثقافي الأول، قسم العلوم السياسية، جامعه القاهرة، ٢٠٠٠.

الذي ظهر في أوروبا ابتداءً من الحرب النابليونية إلى الحرب العالمية الثانية، غير أن هذه الحروب أصبحت هي الاستثناء، كما أن طبيعة التهديدات الإرهابية قد أوجدت نوعاً جديداً من الحروب لا تنطبق عليه اتفاقيات جنيف، بل تجعل تلك الاتفاقيات على نحو ما، وكأن الزمن قد تجاوزها، ومثل هذه المجادلات تشير إلى قدر أوسع من الشك في مدى استخدام اتفاقيات جنيف وآخذاً في الاعتبار تغيير طبيعة الحروب والمشاركين في هذه الحروب.

وأظهرت الثورة التكنولوجية الفجوة بين القواعد القانونية التقليدية وما بين التطور في النظام الدولي، و مع التنامي المستمر في ظاهرة الاعتماد الدولي في بعدة الاقتصادي والأمني والسياسي، وانتقل القانون الدولي من قانون تشكل نواته الدولة إلي مرحلة جديدة بني فيها على فكرة الصالح المشترك للجماعة الدولية ككل ولينتقل من التعبير عن مصالح جماعه دولية محدودة.

وظهرت تحديات غير تقليدية للمجتمع الدولي ولتتسع لتشمل الأمن الإنساني بمفهومه الشامل كحماية حقوق الإنسان ومكافحة التلوث والإرهاب الدولي وقضايا الاحتباس الحراري وغيرها، وتميزت تلك القضايا ببعدها الدولي وتعديها للحدود الوطنية، و طرأ تغير على مفهوم سيادة الدول وعدم التدخل في شئونها الداخلية والحق المشروع في استخدام القوة، وكانت تلك المبادئ تمثل روح القانون الدولي التقليدي ومحور قواعده الدولية،

كما تغيرت طبيعة الحرب والعدوان والإرهاب، ولم يقتصر التطور الذي شهده القانون الدولي في قواعده وأشخاصه بل ظهر أيضا في مجاله. [1] وأصبحت الحروب تتراوح بشدة بين صراعات غير متوازنة تضع جيوشاً مدربة تدريباً راقياً ومجهزه بأحدث الوسائل التكنولوجية، أمام مقاتلين غير نظاميين يركبون الخيول وبين صراعات يتداخل فيها أشباه العسكريين والمجرمين، والطابع المدني بالعسكري وظهرت الحروب الحديثة والمقاتلون الجدد و الاستخدام العسكري للأهداف المدنية، وجاءت اتفاقيات جينيف لتتعامل مع الجيوش التقليدية، بينما تفرض الحروب الحديثة تحديات عدم وجود خطوط قانونية واضحة تحمى هؤلاء الذين يتم القبض عليهم في الصراعات، كما إن هذه الخطوط العريضة لا تحترم من قبل المشاركين في وضعها سواء من الدول أو من غير الدول ومن ضمنهم المحاربين في حرب العصابات والجماعات التي تستغل الأطفال في الحروب. [2]

ودفعت تلك التغييرات لإعادة النظر في اتفاقيات جينيف بشان الأسرى لأنها غير قادرة على التعامل مع تلك التطورات، وأصبح العالم وفقا لوجهه النظر الحربية لم يعد فيه بالضرورة تحارب الدول بعضها البعض، بل أصبح هناك محاربون غير شرعيين دون الدولة ومن ثم لا ينطبق عليهم اتفاقيات جينيف بشان الأسري فالإرهابيون يعاملون كأسري حرب ومن ثم فلهم حقوق الأسرى وفق اتفاقيات جنيف على الرغم من أنهم محاربون غير شرعيين لأنهم ليسوا بأعضاء في جيش نظامي ولا يرتدون زى عسكري. [3]

---

(1) د. إسماعيل صبري مقلد، مرجع سابق ذكره، ص ص ١١-٦٤.

(2) Renee de Never," Modernizing the Geneva Conventions", The Washington Quarterly, Vol. 29, No. 2 Spring 2006.

(3) Renee de Never," Modernizing the Geneva Conventions ,Op.Cit.pp 23-27

وظهرت إشكاليات تتعلق بمسالة تحديد الأهداف المدنية والأهداف العسكرية وتعريف العدوان وتعريف الحرب وحماية المدنيين والأماكن التي تستحق الحماية، وتحديد ضرب الأهداف المشروعة والتمييز بين الأهداف العسكرية والمدنية، ومدى القدرة على تقليل حجم الأضرار وقت الحرب أو التهديد بشان استخدامها، و جاءت التغيرات التكنولوجية بأنشطة جديدة لا يوجد تكييف قانوني واضح يلائمها في الأطر القانونية الحالية أو أنها كشفت عن التعارض ما بين القوانين الدولية القائمة بالإضافة إلى بروز مشكلات تتعلق بوضعها القانوني."(1)

وأصبحت الحرب في العصر الحديث لا تشبه إلا في أقل القليل المعارك التي كانت تدور بين جيوش متكافئة بقدر أو بآخر ويتقابل فيها جنود يرتدون الزى العسكري وينتمون إلى دول بينها عداء، وقد وضعت اتفاقيات جنيف خصيصاً لها، ومسالة تحديد الأهداف المدنية والعسكرية وتعريف العدوان والحرب وحماية المدنيين والمنشآت التي تستحق الحماية، ومدى القدرة على تقليل حجم الإضرار وقت الحرب،و مثل ذلك خطرا على الالتزام بقانون النزاعات المسلحة، وفرض تغييرات في الإطار القانوني والمبادئ التي يقوم عليها ونطاقه ووسائل تطبيقه والأشخاص المحميون والقواعد الأساسية للنزاعات المسلحة والمسئولية المترتبة على خرق القانون وطبيعة الانتهاكات والجزاء والعقاب. ."(2)

وفرض الاستخدام السلبي للتقدم التكنولوجي تحديات في سبيل معالجة القانون الدولي ، وأصبح هناك تأثير متبادل بين التقدم التكنولوجي وما يفرزه من تحديات وقدرة القانون الدولي على التكيف معها (3) ، وأصبح هناك تأثيرات على بنية وتفاعلات العلاقات الدولية بشكل عام، أما الأول فهو الانتقال من فضاء قانوني مبني على أساس الجغرافيا إلى فضاء قانوني يحتوي في أحد أبعاده التحلل من الأساس الجغرافي والارتباط بالفضاء الإلكتروني حيث ينتفي مفهوم الحدود بمعناها الجغرافي.

وترتب على هذا التحول ضرورة إعادة النظر في ثلاثة مفاهيم هي مفهوم السلطة القانونية ومفهوم التأثير والنفوذ ومفهوم الشرعية، و ثانيا: كما هي المتغيرات الداخلية والمتغيرات الخارجية في تفاعل الوحدات الدولية إلى درجة أصبح الاختصاص المحلي والاختصاص الدولي أمراً ليس من اليسير البت فيه. وثالثا: تجاوز الحدود القضائية ويشتمل على المزج ما بين الجرائم والفضاء الإلكتروني بكل أنواعها كتخريب الممتلكات والسرقة و، وكانت الإباحية والمخلة بالأخلاق وممارسة العنف سواء من خلال العنف اللفظي أو توظيف الفضاء الإلكتروني في ممارسة العنف المادي، ومن المجالات التي تأثرت بالثورة التكنولوجية ظهور الفضاء الإلكتروني، وتعرضه للهجمات وممارسة الأعمال العدائية، وحيث تمثل تلك الهجمات "الحرب الرخيصة "، مقارنة بالأسلحة الأخرى وأصبحت بذلك عنصرا جاذبا للدول والجماعات الإرهابية ويناسب حالة الصراع بين أطراف متفاوتة في القوى.

(1)Bryan W. Ellis," The International Legal Implications and Limitations of Information Warfare: What Are Our Options?",**Op. Cit**,pp 4 -10

(2) Anthony M. Helm,(eds) " The Law of War in the 21st Century: Weaponry and the Use of Force", International Law Studies , Volume 82, Naval War College Newport, Rhode Island 2006,pp. 137-166

(3) مصطفي سلامة حسين، " التأثير المتبادل بين التقدم العلمي والتكنولوجي والقانون الدولي "، دار النهضة العربية، القاهرة، ١٩٩٠، ص ص ٥٦-٧٨ .

ثانيا: طبيعة الفجوة التشريعية بين القانون الدولي وهجمات الفضاء الإلكتروني

ترجع صعوبة تطبيق الأطر القانونية الدولية الحالية على هجمات الإرهاب الإلكتروني إلى أن تلك الاتفاقيات جاءت ثنائية وجماعية، وكانت تخاطب الدول المستقلة دون الأطراف من غير الدول، والذين أصبحوا فاعلين في العلاقات الدولية وشكلت تلك الاتفاقيات التزامات على الدول فقط ولم تشكل نفس الالتزام على الأطراف من خارج الاتفاق أو من غير الدول ، وذلك مثل دور المنظمات الإرهابية في استخدام الفضاء الالكتروني في شن الهجمات واستغلالها في استراتيجيتها العدائية ، وهذا إلى جانب استخدام الدول له في نفس الغرض .

وتتميز هجمات الفضاء الالكتروني بأن هناك صعوبة في تحديد أثارها أو نطاقها كما أنها لا تستطيع التمييز في حالة الهجوم ما بين الأفراد والجماعات والمنشآت الحكومية. ولا تملك القوانين الدولية جاهزية التطبيق تجاه هذا الاستخدام ، ويكون للهجمات التي تشن من مصدر محلي لها آثارا عالمية متعددة مع تمدد الفضاء الإلكتروني.

وخاصة أن القانون الجنائي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا الحديثة، لاسيما أن نصوص القانون الجنائي التقليدي وضعت في عصر لم يكن الفضاء الالكتروني فيه قد ظهر ولم تظهر بعد المشاكل القانونية الناشئة عن استخدامه، مما يفرض علي رجال القانون التدخل لمكافحة الجرائم الناشئة عن استخدامه ومواجهة هذا النقص التشريعي مع عدم وجود نصوص خاصة بهذه الجرائم، بعد أن أصبحت عالمية الطابع وظهرت أنماط جديدة منها، وتنفذ عن بعد دون الحاجة للفعل المادي وإنما يمكن أن يكون ذلك إلكترونيا .

وعلى الرغم من أهمية القوانين الوطنية في تنامي إدراك عالمي بخطر هجمات الإرهاب الالكتروني إلا أنها لا تعد كافية على الأقل على المدى الطويل وذلك لان الظاهرة ذات طابع دولي ينتشر عبر شبكات تكنولوجيا الاتصال و المعلومات ، وكانت مبادئ القانون الدولي الإنساني وقت الاتفاق عليها لم يوجد بها ما يسمى بهجمات شبكات الكمبيوتر والفضاء الإلكتروني و ارتكزت فقط تلك الأطر القانونية على حماية الإنسان وقت الحرب والنزاعات المسلحة.

وتأكيداً على ذلك فإننا لا نجد بشكل مباشر اتفاقية دولية تتناول الفضاء الالكتروني واستخدامه في الصراع الدولي ، ففي اتفاقية جينيف عام ١٩٤٩ والتي تحدد مفهوم الصراع المسلح بأنة "أي حالة يتم فيها إعلان الحرب أو أي شكل من أشكال الصراعات المسلحة والتي ربما تظهر بين دولتين أو أكثر من الدول المعترف بها من جانب القانون الدولي العام، بالإضافة إلى ذلك فان البرتوكول الإضافي لعام ١٩٧٧ والخاص بحفظ السلام والأمن الدوليين من الصراعات المسلحة حيث شمل تعريفاً أوسع لكافة أنواع الصراعات المسلحة بما فيها الصراعات غير المسلحة حيث يتم التعويل على طبيعة الصراع وليس الممارسة الفعلية له.

وهذه الطبيعة قد لا تأخذ شكل الإعلان الرسمي له ومن ثم فان القانون الدولي الإنساني يهتم بالمعني الأوسع للأنشطة المرتبطة بالصراعات المسلحة، وقد حددت اتفاقية جينيف لعام ١٩٤٩ والبروتوكولات الإضافية الملحقة بها الصراعات المسلحة بأنها الصراعات التي تنشا نتيجة الخلاف بين دولتين أو أكثر

قد تؤدي إلى حدوث غزو بالقوة العسكرية، ولم يتطرق إلى تحديد كيفية حدوث هذه الصراعات أو مداها حيث يكون هناك نوع من الصراع أيا كان مستواه، وفي هذا السياق فان تعبير القانون الدولي الإنساني في الصراعات المسلحة يمكن أن يتم تطبيقها على نطاق واسع بحيث يشمل إي عمل تقوم به جماعه من الأفراد والتي تنتج عن خطف أو تدمير أو تفجير والتي يمكن اعتبارها من الصراعات المسلحة. وأحدثت هجمات الإرهاب الإلكتروني تغيرا في معنى ومضمون وطبيعة الحرب وبما مثل ذلك من تحديات أمام تطبيق القانون الدولي الإنساني عليها والقانون الدولي لحقوق الإنسان،

وما يتطلب ذلك من إيجاد نظام قانوني يتعامل مع تلك الهجمات أو التهديدات الجديدة ومدى ما تمثله هجمات الفضاء الإلكتروني من استخدام للقوة في العلاقات الدولية ومدى ما يمثله ذلك من انتهاك لمبدأ حظر استخدام القوة في العلاقات الدولية وفقاً لميثاق الأمم المتحدة في مادته الثانية فقرة (٤) وكذلك المادة (٥١) التي تتعلق بحق الدفاع الشرعي عن النفس. تتعلق قواعد القانون الدولي الإنساني بالتطبيق على حالة قيام حرب أو نزاع مسلح بين دولتين أو أكثر وما ينتج عن هذا من أضرار مادية يعمل هذا القانون على الحد من هذا الضرر وفي المقابل يعمل القانون الدولي لحقوق الإنسان تقليديا في حالة السلم ولكن هجمات الإرهاب الإلكتروني يمكن أن تحدث في حالتي السلم والحرب بما يجعل هناك تداخلا بين حالتي السلم والحرب بما يجعل هناك عدم وضوح حول طبيعة الحقوق القانونية التي يمكن أن تنطبق على الدولة التي تعرضت لمثل هذا الهجوم أو الفاعلين في مجتمع المعلومات العالمي،

وأحدثت هجمات الإرهاب الالكتروني تغييرا في مفهوم الحرب حيث لم تعد وفق العرف الدولي عن عنف منظم من قبل الدول وتنظمه وتحتكره الدولة من قبل دول قومية وجيوش نظامية وخضع هذا العنف تدريجيا إلى نواظم عالمية كالجهود الدولية لحماية المدنيين وقت الحرب وحقوق الأسرى والحق برد العدوان وحق الدفاع الشرعي، وظهرت حروب تختلط فيها القوات النظامية بالجماعات السياسية المسلحة والجريمة المنظمة وبما حمل ذلك اختلاف في التنظيم والغايات والأساليب وهي تحمل طابعا محليا وعالميا في ذات الوقت، مما يفرض تحديات في سبيل ملاحقة آثارها وبإبعادها ومدى تورط أطرافها ويفرض كذلك كيفية المواجهة والتي أصبحت ذات طابع عالمي، حيث تنتشر هجمات الفضاء الالكتروني بسرعة عالية، ويمكن أن يشنّها أي شخص على اتّصال بالإنترنت ويستطيع تتبع التعليمات البسيطة.

وربما يؤدي منحى تزايد نقاط الضعف - مقروناً بمدى ملاءمة الهجوم وقدرته على حرمان الخصم من معلومات عن المهاجم - إلى اندلاع حرب المعلومات والإرهاب الالكتروني بمشاركة أفراد ومجتمعات وشركات ودول، وربما تحالفات وتطرح العمليات العدائية والصراع في الفضاء الإلكتروني تساؤلات من قبيل:أولا: ما مدى ما تمثله الأنشطة التي تنشا بين الدول أو غيرها في الفضاء الإلكتروني خطرا أو استخداما للقوة وفقا للقانون الدولي أم أن هذا الاستخدام للقوة يأتي بشكل مختلف عما

تناولته قواعد القانون الدولي[1]، وثانيا متى يتم اعتبار الخطر أو استخدام القوة جزءا من الهجوم المسلح ومدى إمكانية تطبيق قانون النزاعات المسلحة في حالة الدفاع الشرعي في الفضاء الإلكتروني، وهناك منهجان احدهما كمي يرى في هجمات الإرهاب الإلكتروني وحرب المعلومات أنها ترتقي إلى حالة النزاع المسلح وحالة استخدام القوة في العلاقات الدولي، حيث يمكن أن تتشابه في الغايات ولكنها تختلف في الوسائل حيث يمكن لهجوم الفضاء الإلكتروني أن يتسبب في حدوث أضرار على نحو مشابه للهجوم التقليدي ، وبما يمكن تطبيق نفس القاعدة التي تحكم استخدام القوة في العلاقات الدولية.[2]

وهناك "المنهج النوعي " الذي يرى في النشاطات العدائية داخل الفضاء الإلكتروني تدخل ضمن الأنشطة غير العسكرية ولكنها لها صلة بالحرب مثل حالة قطع العلاقات الدبلوماسية وفرض المقاطعة الاقتصادية بالإضافة إلى الأشكال الأخرى من الإرهاب التي يطلق عليها أيضا الصراعات منخفضة الشدة والتي يمكن إن تتسبب في إحداث قتل وتدمير مقارنه بالنشاطات العسكرية، وأصبحت أسلحة الفضاء الإلكتروني لا تتشابه مع الأسلحة العسكرية التي كانت تستخدم في الماضي، فمنذ ٦٠ عاما كان التلغراف يستخدم فقط كوسيلة اتصال، ولكن أصبح البريد الالكتروني يمكن أن يحمل أيضا فيروسا قد يتسبب في تدمير أو إحداث ضرر بالغ، فهجمات شبكات الكمبيوتر تتضمن نوعا من التدمير يكون له نتائج في العالم الطبيعي المادي.

ويمكن النظر لهجمات الإرهاب الالكتروني على أنها نوع أخر من استخدام القوة وفقا للمجال والمدة الزمنية وكثافة القوة المستخدمة والتي يمكن أن ترتقي لحالة الهجوم المسلح. وانه وفق ما استقر عليه العرف والقانون الدولي من أن الهجوم يعني "استخدامها، ، سواء كان هجومياً أو دفاعياً" ومن ثم فان ما تسببه الهجمات من أضرار وآثار مع تعدد وسائل ذلك الهجوم، وتلك الوسائل قد تستخدم بغرض الهجوم أو بغرض الدفاع. ويقف خلف تلك الهجمات فاعلون بما قد يرتب المسئولية القانونية خلف استخدامها ، وتعد هجمات الإرهاب الالكتروني نوعا من أنواع الهجمات مثل الهجمات التي اعتبرها القانون الدولي هجوما مسلحا أو شكلاً من أشكال العدوان. وقد استبدل " ميدان المعركة "، بفضاء المعركة ذو الطابع الالكتروني ليعبر ذلك عن تحول طبيعة الحرب من الاعتماد على الطابع المادي للفضاء الالكتروني، وحدث تغير في طبيعة المقاتلين في الفضاء الإلكتروني حيث يمكن للمدنيين أن يلعبوا دورا متزايدا للانتصار في هذه العمليات، وهناك فقداناً لحالة الحماية الدولية لغير المقاتلين أو للمدنيين وفقا للقانون الدولي الإنساني مع استخدام المنشآت أو الخدمات المدنية في العمل العسكري.

وأصبح التفوق المعلوماتي والقدرة على امتلاك قدرات تطوير أسلحة الكترونية والسيطرة على الفضاء الالكتروني من عناصر النصر ومكوناً أساسياً من إستراتيجية القوة العسكرية عن طريق

---

(1) Michael N.Schmitt," **Computer networks Attack and the use of force in International law: thoughts on a normative Framework** ", The Columbia Journal of Transnational Law, Volume 37, 1999, pp. 885-937.

(2) Thomas C. Wingfield and James B. Michael," **An Introduction to Legal Aspects of Operations in Cyberspace**", Naval Postgraduate School Homeland Security, Monterey, California, 28 April 2004, pp 10-18.

القدرة على جمع المعلومات وعملية نقلها والحفاظ عليها ومنع التعرض للهجمات مقارنه بقدرة الخصم على فعل ذلك، كما يتضمن مفهوم الانتصار في هذه الحرب القدرة على بناء شبكة عمليات متاحة للاستخدام العسكري للفضاء الالكتروني وممارسة عمليات الرصد والرقابة، وضمان تدفق البيانات والمعلومات والحفاظ على عمليات القيادة والسيطرة، والقدرة على الحماية من خطر التعرض للهجوم،و التأثير على عمل البنية التحتية وضمان حرية الحركة للقوات داخل الفضاء الإلكتروني لتشكل معايير انتصار جديدة في حرب من نوع مختلف.[1]

ويفرض ذلك إشكالية تحديد وتمييز ذلك الانتصار أو الدفاع الشرعي عن العدوان وقد أصدرت الأمم المتحدة قرارا في ديسمبر عام ١٩٧٤ عملت فيه على إيجاد تعريف يلقى الكثير من الإجماع للعدوان على الرغم من الاختلافات حول مضمونه [2]، وجاء ذلك انطلاقا من كون أحد مقاصد الأمم المتحدة الأساسية هو أن تصون السلم الأمن الدوليين وأن تتخذ التدابير الجماعية الفعالة لمنع أسباب تهديد السلم وإزالتها، ولقمع أعمال العدوان وغيرها من وجوه الإخلال بالسلم، وقد اعتمد القرار تعريفا للعدوان في مادته (١) بأنه " استعمال القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأية صورة أخرى تتنافى مع ميثاق الأمم المتحد" ويتميز هذا التعريف بإضافة عبارة بأية صورة أخرى تتنافى مع مقاصد الأمم المتحدة بما يعني شمول ذلك التعريف لكافة أنواع العدوان المحددة في المادة أو التي قد تظهر وتحمل عدوانا، ومن ثم فان هجمات الإرهاب الإلكتروني إذا كانت لا تهدد سيادة الدول مباشرة بمفهومها التقليدي فإنها تهدد سيطرة الدول على مرافقها الحيوية والإستراتيجية.

وبما يتضمن ذلك التأثير على مواطنيها سواء من خلال التأثير على الخدمات التي يتم تقديمها أو ما يتعلق بدور الفضاء الالكتروني في ظهور الإعلام الالكتروني الذي هدد احتكار الدولة التقليدي لوسائل الإعلام، وما يكون لذلك من انعكاس على الاستقرار السياسي وما يرافقه من تداعيات أمنية مختلفة، فعندما يتم مهاجمة المواقع الحكومية على الإنترنت أو المؤسسات المالية وتهديد خدمة التجارة الالكترونية، فان ذلك قد يعد نوعا من أنواع العدوان أضافه إلى ذلك ما قد يتضمنه ذلك العدوان من أبعاد ثقافية، تضمن سيطرة واختراق القيم المحلية عن طريق استخدام القوة المرنة،

ولم وتحدد المادة التي تجرم استخدام القوة في العلاقات الدولية نمط هذه القوة وتم التركيز على تداعيات استخدامها، ومن ثم فانه إذا كان ذلك الاستخدام ينتج اثارا من شانها تهديد الأمن والسلم الدوليين فانه حري بالمجتمع الدولي أن يقوم بتجريم استخدام هذه القوة على نحو مباشر وبالتركيز على ما تم تناوله في إطار روح القانون الدولي ومقتضيات السلم والأمن الدولي. كما أكدت المادة (٢) من القرار بان" المبادأة باستعمال القوة من قبل دولة ما خرقا للميثاق تشكل بينة كافية مبدئيا على ارتكابها عملا عدوانيا"، وإذا تم تطبيق ذلك على هجمات الفضاء الإلكتروني واستخدامها في الحرب

---

[1] Rebecca Grant. "**Victory in Cyberspace**", Arlington, VA, Air Force Association, 2007. pp 32.

[2] اعتمدته الجمعية العامة للأمم المتحدة بموجب القرار ٣٣١٤ في جلستها العامة رقم 2319 بتاريخ ١٤ ديسمبر ١٩٧٤

أو الإرهـاب فإنهـا تتميـز بضرباتها الاسـتباقية حيث لا يـتم إعـلان حالـة مـن حـالات الحـرب ويـتم توجيهـه الضربات على نحو فجائي .

وان كانت المادة (٣) من القرار قد حددت الأعمال التي يمكن أن يتم اعتبارها عملا عدوانيا [1]، فان تلك الأفعال المحددة يمكن أن تتم داخل الفضاء الإلكتروني بدلا من الفضاء الواقعي مع ملاحظة تغير البيئة التي يرتكب بها فعل الاعتداء، فمثلا قد تقوم دولة بعملية اختراق لنظم المعلومات والبنية التحتية الحيوية لدولة ما بما يمكنها من السيطرة عليها والتحكم في طريقة عملها أو إحداث ضرر أو عمل يوقفها عن القيام بعملها، كما يمكن أن تقوم دولة أو غيرها من الأطراف بقصف المواقع الالكتروني الحكومية الخاصة بدولة ما بفيروسات وغيرها من الأسلحة التي يمكن استخدامها في الفضاء الإلكتروني.

ويمكن لدول ما أن تفرض حصارا على دولة ما عن طريق قطع كابلات الإنترنت أو التشويش على الاتصالات و منع الدخول أو حجب لمواقع على الإنترنت، كما أن الفضاء الإلكتروني ساعد على أن تكون دولة ما مكان لانطلاق عمل الاعتداء ضد دولة أخرى خارجية مع عملية الربط بين شبكات الكمبيوتر والإنترنت بين دول العالم وتجاوزها للحدود التقليدية وسيادة الدول، ومن ثم أصبحت الدول المعتدية بغير حاجة إلى إرسال عصابات أو جماعات مسلحة، كما إن الدفع بعملية التجسس وتجنيد العملاء قم يتم عبر الفضاء الإلكتروني بهدف اختراق الدول الأخرى.

وقد جاءت المادة( ٤) من قرار الأمم المتحدة لكي تؤكد " أن الأعمال التي تم تحديدها في القرار ليست جامعة مانعة، ولمجلس الأمن أن يحكم بأن أعمالا أخرى تشكل عدوانا بمقتضى الميثاق". بما يفتح المجال إلى إضافة أي مظاهر من مظاهر العدوان إلى تلك الإعمال، وفي المادة (٥) تم التأكيد على أن ما من اعتبار أيا كانت طبيعته، سواء كان سياسيا أو اقتصاديا أو عسكريا أو غير ذلك يصلح أن يتخذ مبرّرا لارتكاب عدوان.كما أنه فان تلك المادة تهدف إلى الحد من أشكال العدوان التي يمكن أن تتخذ مبررا أو تقف وراءها دوافع بعينها. كما أنه إذا ما تم اعتبار هجمات الإرهاب الإلكتروني عدوانا انه يترتب على ذلك مسئولية قانونية إذا ما تم تحديد هوية من يقوم بها وما يكون لذلك من مطالبات قانونية بالتعويض المادي والمعنوي عن آثار هذا العدوان وذلك بعد توافر الإطار القانوني لجريمة العدوان من أساسها وأركانها القانونية [2].

---

[1] كان من ضمن ما حددت المادة من أعمال تدخل ضمن أعمال العدوان: (أ) قيام القوات المسلحة لدولة ما بغزو إقليم دولة أخرى أو الهجوم عليه، أو اي احتلال عسكري، ولو مؤقتا، ينجم عن مثل هذا الغزو أو الهجوم، أو اي ضم لإقليم دولة أخرى أو لجزء منه باستعمال القوة؛ (ب) قيام القوات المسلحة لدولة ما بقذف إقليم دولة أخرى بالقنابل، أو استعمال دولة ما أية أسلحة ضد إقليم دولة أخرى؛ (ج) ضرب حصار على موانئ دولة ما أو على سواحلها من قبل القوات المسلحة لدولة أخرى؛ (د) قيام القوات المسلحة لدولة ما بمهاجمة القوات المسلحة البرية أو البحرية أو الجوية أو الأسطولين التجاريين البحري والجوي لدولة أخرى؛ (هـ) قيام دولة ما باستعمال قواتها المسلحة الموجودة داخل إقليم دولة أخرى بموافقة الدولة المضيفة، على وجه يتعارض مع الشروط التي ينص عليها الاتفاق، أو اي تمديد لوجودها في الإقليم المذكور إلى ما بعد نهاية الاتفاق؛ (و) سماح دولة ما وضعت إقليمها تحت تصرف دولة أخرى بأن تستخدمه هذه الدولة لارتكاب عمل عدوان ضد دولة ثالثة؛ (ز) إرسال عصابات أو جماعات مسلحة أو قوات غير نظامية أو مرتزقة من قبل دولة ما أو باسمها تقوم ضد دولة أخرى بأعمال من أعمال القوة المسلحة تكون من الخطورة بحيث تعادل الأعمال المعددة أعلاه، أو اشتراك الدولة بدور ملموس في ذلك .

[2] إبراهيم زهير الدراجي ،" جريمة العدوان ومدى المسئولية القانونية الدولية عنها "، رسالة دكتوراه ، كلية الحقوق ، جامعه عين شمس ، ٢٠٠٢ ، ص ص ٢٦٠- ٩٦١ .

وساعد انتشار تكنولوجيا المعلومات وعلاقتها المباشرة بالجوانب المدنية والعسكرية إلى اتساع ميدان الحرب لتمتد إلى حرب وهجمات متعددة الأبعاد والتي تشمل الأرض والبحر والمجال الجوي والفضاء الخارجي والالكتروني وتم وصف الأخير بالمجال المعلوماتي، حيث تكون الحرب موجهه معلوماتيا.(1) وكان لتكنولوجيا الاتصال والمعلومات دور في وجود أهداف جديدة وأشكال جديدة ووفرت إمكانية التعرض للهجوم من خلال استخدام شبكات الاتصالات والمعلومات بما أوجد نوعا جديدا من الضرر يستخدمه العدو وذلك دون الحاجة للدخول الطبيعي والمادي لإقليم الدولة وذلك لان الدول تعتمد على الأنظمة الالكترونية بما يجعلها هدفا للهجوم.

وخاصة أن تلك الأنظمة تحمل طابعا مدنيا وعسكريا مزدوجا بما يجعل هناك خلطاً واضحاً بين ما هو مدني وما هو عسكري، ومثلت تلك التطورات تحديا للقانون الدولي لان القانون بطبيعته المحافظة بشكل لم يواكب تلك التغييرات التكنولوجية،وخاصة أن الاعتماد الشديد للمجتمعات والاقتصاديات الدولية على الاتصالات الالكترونية قد فرض إمكانية التعرض الكبيرة لأخطار نابعة من أنظمة الكمبيوتر، وفي نفس الوقت أصبحت جيوش الدول وأنظمتها التسليحية أصبحت عرضة للهجوم وأيضا إمكانية الدفاع من خلالها، وهذا ما شكل تهديدا للمعايير القانونية التي عملت على الحد من استخدام القوة في العلاقات الدولية، وضع إشكالية أن تمتد تلك الأطر القانونية التي استقر عليها المجتمع الدولي لكي يتم تطبيقها على هجمات الإرهاب الالكتروني سواء أكانت خلال الحرب أو الإرهاب أو النزاع المسلح الممتد عبر الفضاء الإلكتروني. وظهرت العلاقة بين الاتصالات الالكترونية وقوانين الحرب.

وأصبحت عملية البحث عن شرعية للاستخدام القوة عبر الفضاء الإلكتروني تشكل تحدياً هاماً للمجتمع الدولي، والذي أصبح يستخدم كوسيط للهجمات على الدول أو الأفراد ويقوم به دول وأفراد وجماعات، ففي حين كان هدف قوانين الحرب هو تقنين حالة الحرب ووضع ضوابط في حالة حدوثها ومحاسبة الدول التي تخالفها قواعدها، فان الأمر أصبح مختلفاً في حالة هجمات الإرهاب الالكتروني حيث تكون تلك الهجمات دون سابق إنذار أو إعلان حالة الحرب من جانب طرف ضد طرف أخر وإنما يكتنفه الغموض حول مسئولية من يقف وراءها(2)

وكانت قوانين الحرب تهدف إلى التمييز بين الأهداف المدنية والعسكرية من اجل تقليل حالة الأضرار، والعمل على تقديم مناطق آمنه وتوفير حصانه ضد مهاجمه المدنيين، وعلى الرغم مما لحق بهذه القواعد من تطور ظهر في تناول القانون الدولي الإنساني لتجريم وسائل الحرب الحديثة وطرق استخدامها كالأسلحة الكيماوية والنووية والبيولوجية، فان ذات القانون أصبح أمام تطور أخر مماثل هو ظهور هجمات عبر الفضاء الإلكتروني، وتعد هجمات الإرهاب الالكتروني وحرب المعلومات من

---

(1) Timoyhy L. Thomas , "Chinese American Network Warfare", Joint Force Quarterly, USA , Issue 38, 2005, pp 76-83.

(2) David J. Gruber," Computer Networks and Information Warfare Implication for Military Operations", Occasional Paper, No. 17, Center for Strategy and TechnologyAir War College, July 2000.

إحدى أنواعها ، ويتم استخدامها في الصراع الدولي الأكثر ديناميكية بخلاف الصراع التقليدي، فاحد الفرضيات التي يمكن أن تحدث وبشكل غير مرئي بان تقوم القوات الخاصة لأي دولة بشن هجمات باستخدام الأسلحة الالكترونية في مهاجمة البنية التحتية المعلوماتية الخاصة بدولة أخرى.[1]

ومدى ما يمثل ذلك من انتهاك للقانون الدولي الإنساني وقانون النزاعات المسلحة، وكيف يمكن أن يطبق في حالة إعلان الحرب ،و أصبح هناك تحدي للقانون الدولي الإنساني والذي يطبق قواعد مختلفة على المنازعات المسلحة تبعا لما إذا كان النزاع ذا طابع دولي أو داخلي، وهذا التمييز قد أصبح غير مجد لاعتبارات قانونية واعتبارات إن الفضاء الإلكتروني قد عمل على تجاوز التمييز ما بين الفعل المحلي والأخر ذي الطابع الدولي بما يؤكد الرغبة في وجود قانون واحد للنزاع المسلح وذلك بسبب أيضا إخفاق النظام القانوني الحالي في معالجة المنازعات التي تضم عناصر دولية وغير دولية[2].

ولا ينطبق قانون لاهاي المتعلق بوسائل وأساليب القتال وإدارة الجيوش في ميدان المعركة على النزاعات المسلحة، كما أن المادة (٣) من اتفاقية جينيف لا تشمل سوى المشاركين في الأعمال العدائية والأشخاص الذين القوا عنهم أسلحتهم لكنها لا تفعل الكثير لتنظيم القتال أو حماية المدنيين من الآثار الناجمة من الإعمال العدائية، كما إن المادة ٣ تخفق في تعيين قواعد فاصلة للتمييز بين الأهداف العسكرية والأهداف المدنية، ولا تشير إلى التناسب عند اختيار الهدف، ورغم من أن البرتوكول الإضافي الثاني يتناول بالفعل حماية السكان المدنيين على نحو أوضح فإن نطاق شموله لا يقارن بحظر الهجمات العشوائية وحظر أساليب ووسائل الحرب التي تسبب آلاما غير ضرورية وحظر تدمير البيئة الطبيعية.[3]

وكان لذلك تأثير على مبدأ التمييز في الحرب وإمكانية تطبيقه عليها، وكذلك طبيعة القيود والالتزامات التي يمكن فرضها على هجمات الفضاء الإلكتروني لكي يتم حماية الأهداف ذات الطبيعة الخاصة وقت الحرب أو النزاع، وكيفية القدرة على تحديد طبيعة النشاط المدني من الحربي وكذلك التمييز بين المحاربين وغير المحاربين وتحديد الأنشطة التي يعد قيامها عملا عدائيا من إعمال الحرب والتي تفقد المدنيين الحماية القانونية، وعلاقة ذلك بالإجراءات التي يمكن أن يتخذها المدافع لكي تدخل ضمن الاحتياطيات ضد الهجوم، والصعوبات التي تعترض تحديد المنشآت واجبة الحماية أثناء الهجوم المسلح في الفضاء الإلكتروني وصعوبة تحديد مشروعيته القانونية [4]

وتتشابه الأضرار التي تنتج عن التعرض لهجمات الإرهاب الإلكتروني وحرب المعلومات مع تلك الأضرار التي تسببها الحرب التقليدية، كما أنها يمكن ملاحظتها في حالة الحرب التقليدية وضمها

---

(1) Mark R. Shulman," Discrimination in the Laws of Information Warfare",School of Law Faculty Publications,Pace University, Columbia Journal Of Transnational Law ,1999,pp 937- 998

(2) جيمس ج. ستيوارت، " نحو تعريف واحد للنزاع المسلح في القانون الدولي الإنساني: رؤية نقدية للنزاع المسلح المدول " المجلة الدولية للصليب الأحمر، ٣١-١٢-٢٠٠٣. يمكن مراجعتها على الرابط التالي (أخر زيارة ٢٠-٩-٢٠٠٨ ) (http://www.icrc.org/web/ara/siteara0.nsf/htmlall/6LDJA6/$File/Identification_IHL..pdf )

(3) جيمس ج. ستيوارت، مرجع سابق ذكره.

(4) Jeffrey T.G. Kelsey.," NOTE Hacking into International Humanitarian Law:The Principles of Distinction and Neutrality in the Age of Cyber Warfare", Michigan law review, Vol. 106, pp 1452-1427( http://www.michiganlawreview.org/archive/106/7/kelsey.pdf)

ضمن أعمال الحرب في حين أن تدمير نظم المعلومات أو إفساد أو تعطيل أو تخريب المعلومات المخزنة أو عملية الانتقال يمكن أن يتسبب في أضرار بالغة وأن قدرة المعلومات أو الإشارات الالكترونية على الانتقال داخل الشبكات الدولية تفرض تحديات تتعلق بالسيادة القومية للدول على أراضيها وأصبح العالم يعتمد بصورة متزايدة على الشبكات التي تعبر الحدود الدولية مع إتاحة الفرصة أمام أي فرد أو فاعل في التأثير في حركتها أو محتواها، وبذلك أصبح مفهوم السيادة التقليدي الخاص بالدولة غير قابل للتطبيق، بالإضافة إلى المبادئ الأخرى من قبيل أن الدولة فاعل رئيسي في العلاقات الدولية وان سيادة واستقلال الدولة ، وعدم التدخل في الشئون الداخلية في الدول الأخرى واحترام استقلالها كل ذلك قد تغير مع تغير البيئة التي أصبح عليها المجتمع الدولي مقارنة بالبيئة التي أفرزت ذلك النظام القانوني .

وأصبحت شبكات المعلومات ونظم الاتصال تخترق حدود الدول بما يعد بالمفهوم التقليدي انتهاكاً لسيادتها، إلا أن المجتمع الدولي والعرف الدولي أصبح لا ينظر إليها كذلك بل أصبحت من مقتضيات الحياة المعاصرة، بما ينعكس على وجود صعوبة في وصف حرب المعلومات وهجمات الإرهاب الإلكتروني "كحرب" كما إن هناك صعوبة في تحديد الأهداف ذات الطابع العسكري والأخرى ذات الطابع المدني التي تخضع لحماية القانون الدولي.[1] وعلى الرغم من أن روح القانون والعرف الدوليين لا تسمحان باستخدام القوة في العلاقات الدولية إلا في نطاق محدود إلا أن استخدام الفضاء الإلكتروني في شن الهجمات جاء كشكل من الاستخدام الجديد للقوة في العلاقات الدولية والذي تميز بسمات وخصائص معينة بخلاف القوة الصبة التقليدية.[2]

و لم يوجد أي إشارة مباشرة لذلك النوع من التهديد الجديد أو السلاح في القانون الدولي الإنساني حيث إن هجوم الإرهاب الالكتروني لا يرتبط بالصراعات المسلحة التي ارتبط بميثاق الأمم المتحدة ومبادئ القانون الدولي، ولم تتطرق اغلب الاتفاقيات الدولية الموجودة إلى ذلك النوع من التهديد الجديد واستخدامه لا يخضع لأي سند قانوني أو اتفاق دولي إلا ما يتعلق بالعرف الدولي والقياس وآراء الفقهاء كمصادر للقانون الدولي .

وأحدثت هجمات الإرهاب الالكتروني ثورة في الصراع المسلح بما هدد بآثار كارثية وانهيار أهداف حيوية داخل منظومة البنية التحتية الكونية للمعلومات، وذلك كون الاعتداء باستخدام الحاسب الآلي هو أي عملية تهدف إلى تعطيل، أو منع، أو إضعاف أو تدمير المعلومات الموجودة في شبكات الحاسب الآلي.، وتعكس إمكانية القيام بمثل تلك الاعتداءات كأداة من أدوات النزاع المسلح الدولي، ويمكن أن تكون عواقبها بعيدة المدى. وهذا ما يطرح علاقة وموقف القانون الدولي الإنساني من هذه الاعتداءات عبر الفضاء الالكتروني وما يكون لذلك من تأثير على قانون إدارة الصراع فيما يعرف بقانون الحرب وهو عبارة عن مجموعه من القواعد تنظم الأفعال القانونية وغير القانونية في أثناء النزاعات المسلحة.

---

(1) LTC Bryan W. Ellis,",Op.Cit.
(2) Bill Hutchinson & Mat Warren ," **Information Warfare : Corporate Attack and Defence in Digital World** ", ,typeser by Avocet typest ,brill,Aylesbury,bucks, Great Bretain , 2001.

واقر القانون الدولي في المادة ٢ فقرة ٤ حظر استخدام القوة أو التهديد بها في ميثاق الأمم المتحدة وظهرت أهمية التعامل مع قضية تطبيق القانون الدولي على المنازعات الدولية إذا ما نشبت في الفضاء الإلكتروني، وكيف يمكن تحديد الأنشطة السلمية والأخرى غير السلمية في ظل تصاعد النمو والتطور التكنولوجي، وما يمكن للدولة أن تقوم بعمل ينطوي على استخدام القوة أو التهديد باستخدامه في الفضاء الإلكتروني، وما هي الحدود التي تفرض على الدولة حيث يتم التركيز على طبيعة الأنشطة التفاعلية بين الدولة التي تعد ذات طابع سلمي، وكيف يمكن أن تتحول إلى أن تشكل تهديداً باستخدام القوة وفقا للقانون الدولي وتعامله مع أداره الصراع وتنظيمه له، ومدى رؤية تلك الأفعال على أنها تشكل تهديدا لميثاق الأمم المتحدة ومدي كونها تشكل نمطا جديدا من" استخدام للقوة " أو"هجوما مسلحا"وفق مفاهيم القانون الدولي [1].

ولم يتم تنظيم استخدام الفضاء الالكتروني في حالة النزاع المسلح ،و لم يتم تناوله بشكل مباشر في مبادئ القانون الدولي الإنساني، والذي يتم توظيفه واستخدامه كوسيلة من وسائل الحرب الجديدة والإرهاب دون أن ينظم ذلك مجموعه الضوابط والقواعد التي يمكن تطبيقها على أطراف النزاع في حالة الصراع الدولي. [2] وهناك جدل حول مدى ملاءمة القانون الدولي الإنساني عمليا للتعامل مع الطرق والوسائل الجديدة للحرب التي تنتج من استخدام الفضاء الإلكتروني، حيث تكون الهجمات خارج نطاق القوة الصلبة التي تتعامل معها القانون الدولي الإنساني، ومن ثم فان القانون الدولي الإنساني يقع خارج نطاق التعامل معها، وبعبارة أخرى فان القانون الدولي الإنساني طبق في حالة النزاع المسلح وفي حين لا تحمل هجمات الإرهاب الالكتروني صفه "النزاع المسلح" كما جاء تعريفة في القانون الدولي أو حتى في حالة تعريف "العدوان".

<u>وتتلخص أهم الإشكاليات في التالي ذكره:</u>

يتضمن القانون الدولي بالأساس احتمالات واقعية مادية سواء في مجرياتها أو نتائجها أو أثارها، كما أنة حتى لو تم تضمين هجمات الارهاب الالكتروني كحالة نزاع مسلح فانه يصعب تصنيفها كحالة هجوم، حيث إن الهجوم على المدنيين أو المنشآت المدنية قد لا يسفر عن وقوع ضحايا أو جرحي وذلك خلاف ما يحدث في الهجوم التقليدي حيث يحظى المدنيين بحماية القانون الدولي، ومن ثم فان هجمات الإرهاب الالكتروني قد لا تعد هجوما بالمعنى التقليدي ودورها في فتح المجال لاحتمال إصابة أشخاص أو أهداف تحظى بالحماية وغير متوقعه ولا يحميها القانون الدولي.

ومن ثم فان الجهود الدولية لإقرار الحماية من التعرض لهجمات الفضاء الالكتروني لا ترقي إلى العمليات الوقائية أكثر من كونها اغاثية، وبما يجعل ذلك هناك تشجيعاً اكبر لتنفيذ الأهداف العسكرية بسهولة مع تقليل حجم الخسائر أو الإصابات العرضية عبر الفضاء الالكتروني بخلاف الهجوم العادي

[1] Walter Gary Sharp "،Cyberspace and the Use of Force ،"Ageis Research Corp ,February 1, 1999.
[2] Thomas C. Wingfield," When is a Cyber Attack an "Armed Attack?"Legal Thresholds for Distinguishing Military Activities in Cyberspace", Cyber Conflict Studies Association, February 1, 2006.

التقليدي، ومن ثم فان ذلك سيمثل إغراءا لاستخدامها من قادة الحرب، وتظهر مسالة الخلط الواضح بين مفهومي الإرهاب والحرب ومن هنا يتم النظر من خلال مدى مشروعية العدوان والحرب.

وقدرة القانون الدولي أن يميز بينهما لكي يتم تطبيق قواعد وأحكام معينة خاصة بها. و يواجه هذا الهجوم تحديات تتعلق بطبيعة الفهم التقليدي لحالة المقاومة لأن استخدام المدنيين للتكنولوجيا ومعرفة كيفية الاتصال بالعمليات العسكرية عن طريق الفضاء الالكتروني من الممكن أن يساعد في انحسار آثار العدوان، أو مدي ما يجب أن يتوافر لهؤلاء المدنيين من حماية تحت حالة الحرب، وأن طبيعة شبكات الاتصال والمعلومات الدولية تفرض قيود على الدول من اجل الخضوع إلى معايير أمان أو حماية وبما قد يتعارض مع سيادتها وحقها في إدارة شئونها الداخلية بدون تدخل خارجي كما قضت بذلك محكمة العدل الدولية بشان نيكاراجوا[1].

وهناك حالة الجرف القاري لبحر الشمال التي أكدت فيها محكمة العدل الدولية على أهمية العرف كمصدر من مصادر القانون الدولي[2].فمنذ اتفاق ويستفاليا ١٦٤٨، والذي أكد على سيادة الدولة المطلقة على كامل أراضيها داخل حدودها المعترف بها دوليا، ولكن أصبح مفهوم السيادة غير ملائم للتطبيق مع درجة التشبيك العالية بين دول العالم، ووجود فضاء الكتروني وعالم شبكي عابر للحدود الدولية والسيادة الإقليمية للدول، وجعلت هجمات الفضاء الالكتروني صعوبة في تحديد مفاهيم السلام والحرب و تحديد الأهداف وطبيعتها المدنية والعسكرية، ويصبح الضرر غير الملموس للإرهاب الالكتروني باعتباره هجوم لا يمكن أن ينطبق عليه القانون الدولي الإنساني أو قانون الحرب الذي هدف على حماية المدنيين، وهناك إشكالية حول تحديد المسئولية القانونية خلف الهجمات، وخاصة أن الدول التي قد تعاني من هجمات الإرهاب الالكتروني قد يصاحبها حالة من التوترات الدولية العالية .

ومن ثم يكون هناك صعوبة في تمييز ذلك الهجوم والتحقق بشأنه، كما انه حتى إذا أخذت الهجمات مجرد رد فعل فإنها قد لا تستطيع التمييز بين الأطراف، ومن ثم فإنها تصبح غير قانونية وذلك لعبور الشبكات الحدود الدولية وإصابة أطراف محايدة، وان التحقيقات بشأن هجمات الإرهاب الالكتروني قد تجمع بين المبادئ الأساسية لعمل أجهزة الاستخبارات كعمل طبيعي مادي وبين الالكتروني العابر للشبكات والحدود الدولية، ولكن عملاء أجهزة الاستخبارات الدولية قد لا يستطيعون الولوج إلى دول أخرى لأنها ستعد ذلك انتهاكاً لسيادتها.

والهجوم الالكتروني قد يأتي من دولة أو من فاعلين من غير الدول ،ويتطلب مواجهته الحاجة لتعاون دولي ،ودعم المساعدة في الحماية ضد الأخطار المشتركة، أو حتى حمل الحكومات المحلية على تقديمها بشأن هجمات كان مصدرها أراضيها، مع عدم وجود اتفاق عالمي حول التعريف القانوني للسلوك الإرهابي وخاصة أن المجتمع الدولي إلي الآن لم يصل إلي تعريف واضح للإرهاب بشكله التقليدي ناهيك

---

(1) عندما تدخلت الولايات المتحدة في نيكاراجوا عام ١٩٨٦ كان راي محكمة العدل الدولية يختلف عن الرأي الأمريكي الذي كان يرتكز على "إن نيكاراجوا اختارت نظامًا شموليًا ديكتاتوريًا شيوعيًا"فقضت المحكمة بان ليس لأي طرف الحق في أن التدخل في اختيار شعب لنظامه السياسي " وعندما ردت الولايات المتحدة الأميركية تقول" إن نيكاراجوا تمتلك أسلحة تهدد بها الأمن في المنطقة" ردت محكمة العدل الدولية بأنه " لا يوجد في القانون الدولي ما يُحد دولة من تملكها لأسلحة ما في غير نطاق المعاهدات الدولية.

(2) .North Sea Continental Shelf Cases, Judgment, ICJ Reports 1969, p. 44, para. 77.

عن الإرهاب عبر الإنترنت فهناك من الدول من يعد الإرهاب سلوكا جنائيا وجريمة والبعض الآخر يعتبر الإرهاب مقاومة مشروعة أو جريمة سياسية.

وهناك تداخل لمفهوم الإرهاب الالكتروني مع غيره من المفاهيم كالجريمة الإلكترونية والمنظمة والاحتيال والتجسس وقرصنة المعلومات وحرب المعلومات وغيرها وفرض ذلك إشكالية تحديد المعاملة القانونية الواضحة ويمثل عنصر المباغتة الذي يتميز به الإرهاب الالكتروني وخاصة في بعده الرقمي تحديا أمنيا ليضع الطرف الأخير في موقف ضعيف حيث يقتصر دوره في تلك الحالة علي رد الفعل مع إصابة الإجراءات الوقائية في مقتل وتطرح مسالة تعدد الفاعلين قضية المسئولية القانونية.

وخاصة أن استخدامه قد لا يقتصر علي الجماعات والأفراد بل قد تستخدمه الدول أيضا ويمثل الفاعلون من غير الدول وخروجا عن الالتزامات القانونية الدولية فكيف يمكن إلزاما الفاعلين الجدد بما تعقده الحكومات الرسمية التي يخاطبها القانون الدولي.، ويضفي البعد الدولي للظاهرة تعقيدا في شأن المواجهة الدولية خاصة مع عدم وجود إطار قانوني دولي واضح لتناول تلك الظاهرة المستحدثة وما يستلزم ذلك إما الحاجة لقانون دولي جديد أو عقد اتفاقيات مكملة للاتفاقيات الدولية أو تفعيل اتفاقيات أخري قائمة.

و يستخدم المهاجمين هذه الهجمات عن طريق نموذج لا مركزي يقوم على ترتيبات الاتصال بين النظراء مما يجعل من الصعب على أي إطار قانوني وطني كان أو إقليمي أن يعالج هذه المشكلة بصورة كافية ولا يمكن التصدي لهذه التحديات البعيدة المدى إلا على مستوى عالمي، وقد اعتمدت بلدان عديدة تشريعات لمكافحة الاستخدام غير السلمي للفضاء الإلكتروني، أو في سبيلها لاتخاذ مثل تلك التشريعات، ويتم اتخاذ مثل تلك التشريعات لكي يتم تنفيذها داخل الحدود الجغرافية للدولة ولكن تبقى هناك صعوبة في حالة إذا ما تم ارتكاب جريمة في مكان أو دولة ما وتم التحريض في دولة أخرى،وذلك ما لم تكن هذه الأطر القانونية قابلة للتطبيق على نحو تبادلي بين البلدان ،ويتم ذلك عن طريق الاتفاقيات الثنائية والتي قد تكون محدودة في تأثيرها، و تظهر بعض التعقيدات بشأن عمليات التفاوض أو عملية توسيع نطاق مثل تلك الاتفاقيات أو اختلاف في المسئوليات المتفق عليها.

ويما يتسبب ذلك في إيجاد ملاذات آمنة للذين يقومون بالاعتداءات عبر الفضاء الالكتروني الذين يحميهم وقوع أنشطتهم خارج الولاية القانونية للدولة أو خارج نطاق قواعد القانون الدولي، ويضاف إلى ذلك أوجه الضعف في تطبيقات البرمجيات والتي تصبح عرضة للفيروسات ،و يستغل المهاجمون تلك الثغرات الأمنية ومهاراتهم في تخطيها، وعدم وجود الهياكل التنظيمية الملائمة، فعندما يقع حادث ما في دول فإن ذلك الأثر لتلك الحادثة قد يصل إلى دولة أخرى. كما إن بعض الشركات أو الحكومات التي قد تتعرض لهجمات الفضاء الإلكتروني قد تخفي حقيقة تعرضا أما خوفا من التأثير على الرأي العام، أو ضعف ثقة المستهلكين أو عدم القدرة على تحديد المسئولية عن تلك الهجمات، وهذا ما يضعف الثقة في الأجهزة الأمنية أيضا.

## المبحث الثاني:
## القانون الدولي الإنساني
## و هجمات الإرهاب الالكتروني في حالة الصراع الدولي

يحاول أن يقدم الباحث في هذا المبحث محاولة إيجاد تكييف قانوني لهجمات الإرهاب الالكتروني وفق ما تم إرسائه من قواعد ومبادئ تحكم حالة استخدام القوة في الصراع المسلح ، ومحاولا – أي الباحث – أن يلمس الخصائص المميزة لاستخدام تلك القوة الجديدة ، وما شكلته من تحدي في سبيل تكييفها قانونيا ، وجاء ذلك عبر استعراض الباحث المطلب الأول بتناول مشروعية استخدام هجمات الإرهاب الالكتروني في حالة النزاع المسلح ، والمطلب الثاني بعرض مشروعية استخدام هجمات الإرهاب الالكتروني في حالة الدفاع الشرعي ، أما المطلب الثالث فيتناول موقف الشريعة الإسلامية ومحكمه العدل الدولية والمحكمة الجنائية الدولية.

### المطلب الأول:
### مشروعية استخدام هجمات الإرهاب الالكتروني
### في حالة النزاع المسلح

لا يتضمن قانون الحرب أية قواعد صريحة بشأن الاعتداءات في الفضاء الالكتروني حيث لا تكون هذه الاعتداءات حركية أي ليست اعتداءات "مسلحة" في حد ذاتها، وينطبق القانون الدولي الإنساني بالفعل بالنظر إلى هدفه الأساسي، وهو حماية المدنيين وممالحرب.. ويكون الهدف من الاعتداء على الفضاء الالكتروني هو تعريض الأشخاص المحميين أو الممتلكات المحمية للخطر – أو المخاطرة بحدوث ذلك – يصبح القانون الإنساني منطبقا وتندرج تلك الاعتداءات تحت قانون الحرب.

وفي مايو عام ١٩٩٩ أصدرت وزارة الدفاع الأمريكية إرشادات حذرت فيها من سوء استخدام هجمات المعلومات والتي يمكن أن تعرض الولايات المتحدة لمسئولية جنائية تتعلق بالاتهام بارتكاب جرائم حرب، وحثت القادة العسكريين على تطبيق نفس مبادئ قانون الحرب .[1] ومن خلال تحليل مشروعية الاعتداءات باستخدام الفضاء الالكتروني من منظور القانون الإنساني، وما يثير ذلك من قضايا قانونية أساسية والمعلقة ذات الصلة بهذا الشأن، خاصة بتعريف "النزاع المسلح" ومقدرة القانون الدولي الإنساني على تنظيم أساليب ووسائل الحرب الجديدة، والمثيرة للجدل من الناحية المفاهيمية، على حد سواء.[2]

ويحاول الباحث جاهدا أن يعمل على تحليل مدى مشروعية استخدام هجمات الإرهاب الإلكتروني أو حرب المعلومات في النزاع المسلح أو في حالة الدفاع الشرعي عن النفس وفق الأطر القانونية الدولية

---

[1] Bradley Graham, "**Military Grappling with Guidelines for Cyber Warfare; Questions Prevented Use on Yugoslavia,**" The Washington Post, 8 November 1999, sec. 1A, p. 6.
[2] Michael N. Schmitt, Wired warfare: Computer network attack and jus in bello , **op.cit**

الحالية ويثير ذلك مدى إمكانية إن تكون لتلك المبادئ علاقة في حال تطبيقها على هجمات الفضاء الالكتروني والتي تنتهي بنتيجة مفادها عدم شرعية استخدامها في حالة النزاع المسلح وتتعلق المبررات النظرية والعملية في التالي:

١- مبدأ تقييد حقوق المتحاربين في استخدام أسلحة الحرب في النزاع

انطلاقا من تغير طبيعة الحرب ومداها ومجالها فان القيود التي يجب إن توضع على المتحاربين أثناء النزاع المسلح يجب أن يتم زيادتها تلافيا للضرر الذي يمكن أن يصيب غير الهدف المقصود سواء من الأشخاص أو المنشآت المدنية أو ما يمكن أن ينتج من خسائر عرضية، خاصة مع تزايد الترابط بين دول العالم من خلال شبكات الاتصال والمعلومات وتدخل ذلك في عمل منشآت حيوية وبنية تحتية كونية يصبح من شان إلحاق الضرر بها إحداث خسائر مدمرة للأمن الإنساني.

وأي سلاح لم يتم ذكره في أية اتفاقية لا يعني بالضرورة إباحة استخدامه، ويعد المثال الواضح للحظر الوقائي الوحيد هو ما ورد في البرتوكول الرابع لاتفاقية الأسلحة التقليدية لعام ١٩٨٠ الخاص بحظر استخدام أسلحة الليزر المعمية والذي الحق باتفاقية عام ١٩٩٥ وهذا السلاح تم تحريمه بمجرد بدء التجارب علية وقبل وضعه موضع الاستخدام العسكري الفعلي، لكن هذا المثال لا يمكن تعميمه لأن معظم التجارب على الأسلحة الجديدة تعتبر أسرارا عسكرية، وبالتالي من النادر التعرف على أثار تلك الأسلحة ومن ثم يصبح تحريم استخدام سلاح معين يأخذ حيزا من الجهد والوقت والنوايا الحسنة وهذا ما قد لا يتوافر، أو يتم التحقق من صحته.

وتم التركيز في اتفاقية جينيف لعام ١٩٤٩ على حماية الأشخاص في حالة الحرب دون الإشارة إلى هجمات الإرهاب الالكتروني، ودون الإشارة إلى استخدام أسلحة معينه، وتناولت البرتوكولات الإضافية عدداً من طرق ووسائل الحرب بصفة عامه، لذلك تعد البرتوكولات الإضافية أكثر ملاءمة لتقديم خريطة عمل للموقف من استخدام هجمات الإرهاب الالكتروني، وتمت الإشارة بشكل واضح في المادة ٣٦ للبروتوكول الإضافي الأول إلى تبني واضعي تلك المادة التطورات الحديثة في وسائل وطرق القتال والتي نصت على أن" يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو إتباع أسلوب للحرب، بأن يتحقق بما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول" أو أية قاعدة أخرى من قواعد القانون الدولي"[1].

وبذلك فقد أقرت تلك المادة حقيقة أن أي نشاط عسكري معين يرتبط بطرق الحرب لم يتم تنظيمها بشكل دقيق فان ذلك لا يعني أنة يمكن استخدامها بدون أي قواعد، ولذلك فان الأشكال الحديثة لهجمات الإرهاب الالكتروني وحرب المعلومات، والتي لم يتم تضمينها في استخدامات الأسلحة التقليدية في الاتفاقيات الدولية ترتبط وتخضع للقانون الدولي الإنساني كأي سلاح جديد عندما يتم استخدامه

---

[1] Knut Dörmann," Computer network attack and international humanitarian law", The Cambridge Review of International Affairs "Internet and State Security Forum", Trinity College, Cambridge,UK,19 May 2001.
(www.icrc.org/Web/eng/siteeng0.nsf/htmlall/68LG92/$File/ApplicabilityofIHLtoCNA.pdf,)

في النزاع المسلح، فإحدى القواعد الأساسية للقانون الدولي الإنساني تقر بأن حق أطرف النزاع في اختيار وسائل وطرق القتال ليس مطلقا "كما جاء في المادة ٣٥ فقرة ١ من البرتوكول الإضافي الأول.

ويتم توجيه هجمات الإرهاب الالكتروني للعدو أو الخصم وذلك بهدف تحقيق أضرار، وهذا ما يجعلها طريقة ووسيلة للحرب، وخاصة أنها تتميز بقدرتها الفائقة على تعدى الحدود الدولية وسرعه تنفيذها وعدم القدرة على تحجيم أثارها وكذلك تحديد حجم المسئولية القانونية للدولة خاصة وانه قد يستخدمها أشخاص مدنيين خارج نطاق القوات المسلحة أو فاعلون من غير الدول .

٢- مبدأ حظر الآلام التي لا مبرر لها

تعتمد البنية الأساسية الحرجة في الكثير من الدول في عملها على شبكات تكنولوجيا الاتصال والمعلومات والتي تتراوح ما بين الاتصالات إلى خدمات الطوارئ ومن الصفقات المالية إلى العمليات العسكرية والخدمات الحكومية والتجارة الالكترونية والاقتصاد الرقمي، ويعكس ذلك الارتباط الشديد بين الطابع المدني للفضاء الالكتروني وإمكانية تعرضه للخطر بما يسبب أضرار اقتصادية وسياسية واجتماعية.،

ومن ثم فان استخدام هجمات الإرهاب الإلكتروني من شأنه أن ينتج عنه آلاما مفرطة بما يتنافى مع الاتفاقيات الدولية التي حظرت استخدام الأسلحة التي تسبب آلاما لا مبرر لها، وبالرغم من عدم تحديد الفضاء الالكتروني كمجال لذلك التحريم إلا إننا يمكننا القياس على ما ورد في تلك الاتفاقيات بما يمكن أن ينتج عن استخدام الإرهاب الالكتروني لإصابة أي بني تحتية حيوية تشكل مصلحة للمجتمع الدولي قاطبة، ولا تختلف عن نتائج استخدام القوة والعمل العسكري التقليدي، حيث أن هناك اختلاف في الآليات العدائية ولكن تتشابه في الآثار والنتائج عبر استخدام أسلحة الفضاء الالكتروني المتنوعة.

٣- مبدأ التمييز بين المقاتلين وغير المقاتلين وما بين المنشآت المدنية والعسكرية

أصبحت مبادئ التمييز تشهد توسعا في تعيين الأهداف العسكرية والتي كانت تعد هي الأهداف المشروعة للحرب وفق القانون الدولي، ولكن عندما يتم تطبيق ذلك على هجمات الفضاء الإلكتروني فان هناك تغيرا في مجال وأهداف الصراعات المسلحة، وحدث هناك تداخل ما بين الاستخدامات المدنية والعسكرية حيث إن كليهما يرتبط عبر شبكة واحدة ووسيط واحد هو الفضاء الالكتروني ، كما إن طبيعة الاستخدام ليست ثابتة ومتحركة ومتداخلة، ومن ثم فان هناك صعوبة في تحديد الأهداف العسكرية التي قد تكون هدفا للحرب.

وظهر مفهوم حديث للحرب يواجه بتحدي تعريف الهدف العسكري، وذلك لان طبيعة الحرب قد تغيرت بشكل كبير ومن ثم فان استخدام هجمات الفضاء الإلكتروني يمكن إن تعمل على اتساع مجال الحرب ونشر أسلحة الفضاء الإلكتروني وذلك مقارنه بالقواعد الأخرى التقليدية التي تقيد انتشار واستخدام الأسلحة التقليدية وحدث تطور مماثل في أساليب القتال والحرب وجعلها متعدية الحدود والمكان والزمان، ولو كان ذلك خارج نطاق العمليات العسكرية، واقتضى هذا التطور وضع القواعد والأحكام التي تكفل حماية المدنيين والأعيان المدنية ضد أخطار الحروب وأضرارها، من

خلال وضع القيود والضوابط التي يستعان بها في التمييز بين الأهداف العسكرية والأعيان المدنية وبين المحاربين وغير المحاربين، ففي حرب الإرهاب الالكتروني تصبح مسألة التفريق بين من يقاتل أو من لا يقاتل صعبة حيث لا يوجد أسرى أو جرحى بل يوجد مرافق وأنظمة لا تعمل أو دمار ذاتي من دون تدخل مباشر كالقصف والتدمير التقليدي. ومن ثم فان تحديد مفهوم "الهجوم" يشكل أهمية قصوى لمعرفة كيفية تطبيق القواعد الخاصة بمبدأ التمييز والقوانين التي تعطي الحماية الخاصة لأهداف ومنشآت معينه. وفي المادة ٤٩ من البرتوكول الإضافي الأول ( فقرة ١) يعرف "الهجمات" أعمال العنف الهجومية والدفاعية ضد الخصم"، وأشار البرتوكول الأول إلى تعريف "أعمال العنف " والتي تتضمن استخدام القوة الطبيعية لذلك شمل مفهوم "الهجمات " أشكالاً أخرى كالوسائل غير طبيعية كالحرب النفسية والسياسية والاقتصادية، وبناء على فهم ذلك والتمييز بينة وبين غيرة من المصطلحات فإن هجمات الإرهاب الالكتروني والتي تستخدم الفيروسات والدود والقنابل المنطقية والبريد المتطفل وشل الخدمة والبريد الدعائي وغيرها.

وبما تعد به نوعا من أنواع الهجوم يمكن أن يسبب أضراراً ملموسة للأشخاص أو لمنشآت حيوية يقف من ورائها برنامج كمبيوتر أو هجوم معلوماتي والتي يمكن أن تصنف كنوع من "أنواع العنف "، وهذا النوع من الهجوم يدخل ضمن اختصاص القانون الدولي الإنساني، كما قد يشمل هجوم الإرهاب الالكتروني نوعا من الحرب النفسية أو سرقة أسرار ونشر إشاعات كاذبة أو تعطيل عمل مؤسسات المال والأعمال ومن ثم فانه إذا ما اعتبرنا ذلك يمثل هجوم مسلح فإنها ستخضع لما قرره البرتوكول الإضافي بشان الهجوم والذي اقر في المادة "٤٨" ٥١ (٢)، ٥٢ من البرتوكول الإضافي الأول والتي تقر بالالتزام بالهجوم المباشر ضد الأهداف العسكرية وتجنب التعرض للمدنيين والأهداف المدنية،

٤- مبدأ: حظر الهجمات العشوائية

إن الهجمات العشوائية "هي التي من شأنها أن تصيب الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز وأقرت المواد ٨- ٥١- ٥٧ من البروتوكول الإضافي الأول لاتفاقيات جينيف لعام ١٩٧٧ على حظر الهجمات العشوائية التي لا توجه إلى هدف عسكري محدد أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن إن توجه إلى هدف عسكري أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر أثارها على النحو الذي يتطلبه البرتوكول، ومن ثم فان من شانها أن تصيب في كل حالة كهذه الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز حيث أن طبيعة تلك الهجمات لا تمتلك التمييز بين ما هو مدني وما عسكري.[1]

وحظر الهجمات العشوائية جرى التأكيد عليها في المادة ٥١ (٤) من البرتوكول الإضافي الأول حيث إن الهجمات العشوائية هي تلك الهجمات التي لا تستهدف هدفا عسكرياً محدداً، أو ذلك الهجوم الذي لا يمكن التحكم في أثارة أو التبؤ بتداعياتها، والمادة ٥١(٤) و٥١(٥) من البروتوكول الأول وتعدد خمسة أنواع من الهجمات العشوائية، وهي: ١) تلك التي لا توجه إلى هدف عسكري محدد، ٢) التي

---

(1) البرتوكول الإضافي الأول ، اتفاقية جينيف ،.١٩٧٧.

تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد ، ٣) لا يمكن حصر آثارها على النحو الذي يتطلبه البروتوكول، ٤) تعالج عدداً من الأهداف العسكرية الواضحة التباعد والتميز بعضها عن البعض الآخر والواقعة في منطقة حضرية، على أنها هدف عسكري واحد ، ٥) تنتهك مبدأ التناسب بين الميزة العسكرية وخسائر المدنيين.

وتبعد تلك القواعد في حال تطبيقها على هجمات الإرهاب الالكتروني والتي ربما تمثل عملية استخدامها أكثر خطورة، وتبقى مسألة توجيه هجمات الإرهاب الالكتروني إلى أهداف محددة شيء غير متوقع أو يمكن التحكم بة وفي نتائجه على الأهداف المدنية وغير المدنية كذلك، حيث تتميز تلك الهجمات باتساع مجالها وكارثية نتائجها وتميزها بعشوائية الإصابة ،

فمثلا عندما يتم إطلاق هجوم من الفيروسات على أنظمة الكمبيوتر لدولة مستهدفة مع بعد تلك الهجمات عن الدول المحايدة أو الصديقة، فان ذلك الهجوم سيوضح الترابط الكبير بين شبكات الكمبيوتر ذات البعد العسكري والأخرى ذات البعد المدني، ومن ثم فان تلك الهجمات ستتصف بالعشوائية كما يصعب التحكم في نتائجها والتي يجرمها القانون الدولي الإنساني. كما اقر بذلك البروتوكول الإضافي الأول، وشمل الهدف العسكري كلا من المقاتلين والمنشآت ووسائل النقل العسكرية والمواقع العسكرية والمواقع ذات الأهمية التكتيكية ، أما الهدف المدني فيشمل المدنيين والمنشات المدنية بجميع أشكالها ووسائل النقل المدنية.

وقد كشفت الهجمات التي تعرضت لها استونيا في مايو ٢٠٠٧ و إبان الحرب الجورجية الروسية في أغسطس ٢٠٠٨ بأنها كانت غير تميزية حيث أنها وجهت إلى خطوط الاتصالات عن طريق توجيه المئات من القنابل "الميجابيت "، وهذا الهجوم لم يتعرض للسكان فقط بل انه اثر على توقف أرقام الطوارئ التي تستخدم في استدعاء الإسعاف وخدمات المطافي لما يزيد على ساعة والتي تقع ضمن المنشآت المحمية وفق القانون الدولي.

<u>٥- حماية الأهداف المدنية والمنشآت التي تحتوي على خطورة خاصة</u>

تشمل حماية الأشخاص من التعرض لآثار النزاع المسلح والمنشات المدنية وذات الطبيعة الخاصة والتي تتعلق مثلا بسير الاتصالات في العالم أو أقمار الاصطناعية أو شبكات الإنترنت، وان هجمات الإرهاب الالكتروني ستوسع من مجال الأهداف الشرعية وذلك لأنها ستتضمن هجوماً مع تأثيرات غير متوقعه ضد الأهداف غير المستهدفة قانونا ، فالهجمات يمكن فقط أن يتم توجيهها إلى الأهداف العسكرية وان تلك الأهداف يجب أن تحمل صفات الهدف العسكري، والتي لا يتم الاعتماد على تحديده تبعا لوسيلة الحرب المستخدمة.

ففي المادة ٥٦ من البرتوكول الإضافي الأول والخاصة بحماية الأشغال الهندسية والمنشآت المحتوية على قوى خطرة، تقر بان " لا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة ألا وهي السدود والجسور والمحطات النووية لتوليد الطاقة الكهربية محلاً للهجوم، حتى ولو كانت أهدافاً

عسكرية، إذا كان من شأن مثل هذا الهجوم أن يتسبب في انطلاق قوى خطرة ترتب خسائر فادحة بين السكان المدنيين.[1]

و لا يجوز تعريض الأهداف العسكرية الأخرى الواقعة عند هذه الأشغال الهندسية أو المنشآت أو على مقربة منها للهجوم إذا كان من شأن مثل هذا الهجوم أن يتسبب في انطلاق قوى خطرة من الأشغال الهندسية أو المنشآت ترتب خسائر فادحة بين السكان المدنيين. وتعتمد تلك المنشآت على أنظمة الكمبيوتر والشبكات في تشغيلها وعلى الفضاء الالكتروني بصفه عامة، وسمح ذلك بإمكانية تعرضها لخطر وقف العمل باستخدام هجمات الإرهاب الالكتروني، ومن ثم فان تعرض تلك المنشآت لتلك الأخطار يمثل انتهاكا لما ورد في روح تلك المادة وهو الحفاظ على تلك المنشآت من أن تكون عرضة لأي هجوم.

كما أن إصابة تلك المنشآت سيمثل انتهاكا لحماية البيئة التي أقرتها المادة ٥٥ من البرتوكول الإضافي الأول والتي أقرت بأن " تراعى أثناء القتال حماية البيئة الطبيعية من الأضرار البالغة واسعة الانتشار وطويلة الأمد. وتتضمن هذه الحماية حظر استخدام أساليب أو وسائل القتال التي يقصد بها أو يتوقع منها أن تسبب مثل هذه الأضرار بالبيئة الطبيعية ومن ثم تضر بصحة أو بقاء السكان"، عندما تعتمد مصانع الكيماويات أو محطات الطاقة النووية على أنظمة الكمبيوتر فان تعرضها سيمثل تلوثا شديدا للبيئة وللسكان المدنيين.

٦- حماية وسائل النقل والتي يتم استخدامها من قبل المدنيين.

كما كان للحرب التقليدية بنية تحتية يتم الاعتماد عليها بالإضافة إلى ما نصت علية قانون الحرب من حماية لوسائل النقل التي يستخدمها المدنين كالبنية الأساسية للسكك الحديدية أو الحافلات، ولكن في حالة هجمات الإرهاب الالكتروني فأنها تعتمد على وسائل تستخدم اغلبها في الشأن المدني ككابلات الاتصالات ومحطات البث ووصلات الإنترنت والتي يمكن اعتبارها من المنشآت المدنية ويجب حمايتها بل أنها من المنشآت التي تتطلب حماية خاصة كتلك التي تناولها القانون الدولي بشأن حماية المنشآت التي تحتوي على مواد خطرة.

كما أن القانون الدولي للبحار لعام ١٩٨٢ قد تناول حماية الكابلات البحرية والتي يمر بها ٩٥٪ من اتصالات المجتمع الدولي وشبكة الانترنت، ففي الفرع الرابع من البحار والذي اعتمد في يونيو ١٩٩٤ وتنص في الفقرة (٣٧) " يجب أن يسهر المحاربون على تجنب الإضرار بالكابلات وخطوط الأنابيب المركبة في قيعان البحار التي لا تعود بالفائدة على المحاربين وحدهم "[2]

٧- الاحتياطيات أثناء الهجوم وواجبات القادة في الميدان

وتعني أن المتحاربين أو أطراف النزاع يجب أن يتخذوا جميع الاحتياطات الممكنة عند تبني وسائل وأساليب الهجوم، بل يجب تجنب إحداث الخسائر في أرواح المدنيين أو إلحاق الاصابه بهم أو الإضرار

---

[1] نخبة من المتخصصين والخبراء "دراسات في القانون الدولي الإنساني"، تقديم د.مفيد شهاب، الطبعة الأولى، دار المستقبل العربي، القاهرة ٢٠٠٠.

[2] دليل سان ريمو بشأن القانون الدولي المطبق في النزاعات المسلحة في البحار، المجلة الدولية للصليب الأحمر، ٣١-١٢-١٩٩٥، يمكن زيارتة على الرابط التالي ( http://www.icrc.org/web/ara/siteara0.nsf/html/5QZKNH)

المدنية، و إن يمتنع الطرف المحارب أو يلغي أو يعلق أي قرار يتعلق بشن هجوم قد يتم توقع نتائجه بصورة عرضية أو إن يحدث خسائر في أرواح المدنيين والأعيان المدنية أو إن يحدث خلطا من هذه الخسائر والإضرار، وان يتم توجيه إنذار مسبق في حالة الهجوم، وان يكون الهدف العسكري ممكنا بين عدة أهداف تلاشيا لإصابة المدنيين.

وفرضت قابلية استخدام الفضاء الالكتروني لمثل تلك الأنشطة العدائية بعض التعقيدات بخصوص الإجراء الاحتياطي الواجب اتخاذه في إنشاء الهجوم والذي ورد في المادة ٧٥ من البرتوكول الإضافي والتي تتطلب انه في حالة الهجوم يتم الالتزام مبدئيا باتخاذ كافة الإجراءات في شكل اختيار وسيلة وطريقة الهجوم والتي يمكن من خلالها تجنب الإضرار وتقليصها التي قد تصيب المدنيين وإمكانية الحد من الأضرار، وهذا ما يجعل هناك صعوبة في ممارسة ذلك الهجوم، كما أن تشابك شبكات الاتصالات والمعلومات يجعل من الصعوبة التمييز بين ما يعد أنظمة مدنية و أخرى عسكرية وبالتالي معرفة الأهداف العسكرية والتي يكون استهدافها قانونيا، والأهداف المدنية والتي يجب أن تبقى بعيدا عن الهجوم إذا ما سلمنا فرضاً مشروعية استخدام هجمات الإرهاب الالكتروني

٨- حظر الانتقام والعدوان غير المباشر

تتضمن إعمال الانتقام استخدام القوة المسلحة من اجل ممارسة أعمال الإكراه المخالفة في حد ذاتها لقواعد القانون الدولي العام ضد دولة أخرى سبق أن ارتكبت عملا غير مشروع، ومن ثم فان أعمال الانتقام أن كانت في حد ذاتها غير مشروعه إلا أنها قد تكون غير ذلك ، إذا كانت بهدف العمل على احترام الشرعية الدولية، وقد تكون تلك الأعمال ذات طابع عسكري وغير عسكري، كما إن مفهوم القوة التي تشكل عدوانا قد تم حصره فقط في استخدام القوة المسلحة سواء مباشر أو غير مباشر.

ولم يشر قرار التعريف إلى أن التهديد باستخدام القوة عمل من أعمال العدوان كما لم ترد الإشارة إلى العدوان غير المباشر ولا العدوان الاقتصادي، فالعدوان غير المباشر قد ينصرف إلى كافة أنواع التدخل في شئون الدول الأخرى غير المشتملة على استخدام القوة المسلحة بما يخالف المبادئ المعلنة في ميثاق الأمم المتحدة، وقد عرفت وثائق الأمم المتحدة عبر الجمعية العامة استخدام القوة بأنه "كل عدوان يرتكب بصورة غير علنية مهما كانت الأسلحة المستخدمة "، واستعمال تعبير العدوان على بعض الصور الخطيرة لاستخدام القوة المسلحة بطريقة غير مباشرة إذ نصت المادة ٣- ٧ "على انه يعتبر من قبيل إعمال العدوان قيام الدول بإرسال عصابات أو جماعات مسلحة أو قوات غير نظامية أو مرتزقة تقوم ضد دولة أخرى بعمل من أعمال القوة المسلحة يكون على نفس درجة الخطورة التي ورد ذكرها أو إشراك الدولة بدور ملموس في ذلك " .

٩- مبدأ المشاركة المباشرة في الإعمال العدائية

حددت المادة ٥٢ فقرة ٣ الظروف والشروط التي يفقد فيها المدني صفته المدنية ليدخل ضمن قانون الحرب باعتباره مقاتلاً، وتعد حماية الصفة المدنية لها أهمية خاصة لان من شأنها المساعدة في الحد من إلحاق الأضرار بالمدنيين والمساعدة في جعل الأهداف العسكرية مباشرة للهجوم، كما عرفت المادة ٥٠ الأشخاص المدنين والسكان المدنين، ولكن هذا المادة قد لا تجد مجالا للتطبيق وذلك لصعوبة الفصل

بين إذا كان مدنياً أم عسكرياً، فقد يمتلك الفرد خبرة بالكمبيوتر وقد يشارك في الهجوم ولكنه لا يحمل صفه عسكرية رسمية تابعه للدولة، وكذلك فقد يساهم بعض الخارجيين عن نطاق دولة ما في دعم موقفها إزاء دولة خصم وهذا ما قد يساعد على فقد ذلك المدني صفته المدنية والحماية من الهجوم وذلك باعتبارها مشاركة مباشرة من المدنين في الهجوم.

وهذا ما يتطلب معرفة من المتسبب في الضرر أو من استخدم هجمات الإرهاب الالكتروني كشكل من "التطبيق المباشر للتدمير الالكتروني بدافع تحقيق هدف عسكري، واجمع عدد من الفقهاء على اعتبار إن استخدام الوسائل الالكترونية كهجمات شبكة الكمبيوتر يمكن اعتباره مشاركة مباشرة في الأعمال العدائية، وهناك من رأي أن اعتبار هجمات الفضاء الالكتروني واستخدامها في الإعمال العدائية لا تعد مشاركة مباشرة في القتال إلا إذا ما نتج عنها الموت أو جرحى أو ضرر طبيعي "، وهناك رأي أخر اعتبار أن هجمات الإرهاب الالكتروني لكي يتم اعتبارها مشاركة مباشرة في القتال يجب أن تتوافر صفة التعمد، وهناك من رأي أن ذلك يخضع لطبيعة الموقف، ومسألة استخدام أسلحة الفضاء الالكتروني يمكن أن تضر بمصالح المجتمع الدولي بما يجعل الإنسانية هي محل الاعتداء، وخاصة عند استخدام أنظمة التسلح ووسائل الاتصالات ووسائل وطرق المواصلات والشبكات الالكترونية في العمليات العسكرية، وتعدحالة مشاركة مباشرة في الأعمال العدائية.

<u>١٠- تهديد الجنس البشري</u>

لقد استطاعت عقدة الصناعة الحربية أن تجعل البحث العلمي رهن إشارة الحرب من أجل ضمان كفاءات الهدم المتبادل. كما أنه بواسطة تطور المعلوماتية والبيوتقنية استطاعت علوم الحياة في نفس الوقت أن تهدد النوع البشري، ليس كما كان بواسطة الإشعاع الذري وإنما عن طريق التلقيح السياسي. وعليه فإن مراقبة وضبط مصادر الحياة هي أصل بقاء الفرد، حين يصبح التهديد لا يهم مجموعة بشرية بعينها وإنما النوع البشري برمته

وأصبحت تشكل المعلومة البعد الثالث للمادة وبعد الكتلة والطاقة ودخلت تكنولوجيا الاتصال والمعلومات مجالات البنية التحتية الكونية للمعلومات كمحطات الطاقة والمياه والسدود والمحطات النووية التي أصبحت ماسة ببقاء ومعيشة الإنسان، ومن ثم فان تعرضها للتهديد لا يعني إلا إنتاج أنواع جديدة من الهدم لتطوير سلسلة من الحوادث الإرادية تضر بمصلحة وبقاء الانسان حيث يتم التعرض لحرب المعلومات والارهاب الالكتروني وبنفس الطريقة يمكن للمعلومة المتوفرة أو غير المتوفرة ألا تكون سرية ما دام كل هجوم أو حادثة متساوية من حيث الوقوع.[1] وهذا ما يتسبب في إحداث أضرار بالغة للمجتمع الدولي أو التسبب في خسائر اقتصادية وانعكاس ذلك على امن المجتمع الدولي .

---

[1] بول فيريليو" القنبلة المعلوماتية"، ترجمة: عادل حدجامي، سعيد توبير، مجلة فكر ونقد، العدد ٢٩، ٢٠٠٦
(http://www.fikrwanakd.aljabriabed.net/n29_14hajjami.htm )

١١- حماية المنشآت ذات الطبيعة الخاصة

إن القانون الدولي الإنساني اقر بوجوب حماية المنشآت ذات الحماية الخاصة، كمحطات الطاقة والمنشآت التي تحتوي على مواد خطرة أو المناطق الأثرية، ولقد أحدثت الثورة التكنولوجية تغيرا في شأن اعتماد عدد من البنية التحتية الحيوية على الكمبيوتر والتحكم المركزي من خلاله، و فرض القانون الدولي الإنساني حماية للمنشآت المدنية و التي تحتوي على خطورة خاصة بالمفاعلات النووية أو مستودعات المواد الكيماوية، والتي تعمل هجمات الارهاب الالكتروني على إصابة تلك المنشآت بما يتسبب في كوارث بيئية وإنسانية.

وذلك مثل المطارات أو خطوط السكك الحديد أو محطات الطاقة وأنظمة الاتصالات والمصانع والتي قد تحمل استخدامين أحدهما مدني والأخر عسكري فقد تستخدم مثلا الأقمار الصناعية مثل انتلساتIntelsat أو اوروسات eurosat أو عربسات Arabsat وتنتقل من الاستخدام المدني إلى الطابع العسكري ، وهذا ما يتوقف على إذا كان ذلك الهدف يحمل طابعا عسكريا ينفي عنه الطابع المدني ومن ثم يتم سحب الحماية المدنية القانونية.، وكذلك يتوقف على طبيعة الصراع فقد يستخدم المجال الجوي في عملية الدعم العسكري ولكنة لا يحمل طبيعة عسكرية خالصة

١٢ – الفئات التي لا تتمتع بوضع أسرى الحرب

أما بالنسبة إلى المشاركين في عملية الهجمات عبر الفضاء الإلكتروني فقد لا يتم اعتبارهم مدنيين على الرغم من نفي صفة العسكرية عنهم إلا أنهم يكونوا اقرب إلى توصيف الجواسيس أو المرتزقة والذين لا يعاملهم القانون الدولي معاملة الأسرى وهم أولا الجواسيس: وهم من يقومون سرا باللجوء إلى بعض مظاهر الخداع بجمع المعلومات العسكرية في الأراضي الخاضعة لسيطرة العدو ويشترط ألا يكون مرتديا للزى العسكري للقوات المسلحة التي ينتمي إليها " كما لا يتم معاملة الجاسوس كأسير حرب وفق المادة ٤٦ من البرتوكول الإضافي الأول لعام ١٩٧٧.

أما الفئة الثانية فهم المرتزقة وهم من جنسية مختلفة عن جنسية الدولة التي يتدخلون فيها، وقد تطرقت المادة ٤٧ من البرتوكول الأول لعام ١٩٧٧ الملحق باتفاقيات جينيف لعام ١٩٤٩، حيث لا يحق للمرتزقة التمتع بوضع الأسير أو المقاتل حيث هم من يجري تجنيدهم خصيصا مرحليا أو في الخارج للمشاركة في القتال في النزاع المسلح ويشاركوا فعلا في الأعمال العدائية وليسوا من رعايا طرف في النزاع وليسوا أعضاء في القوات المسلحة لأحد إطراف النزاع وليس موفدا رسميا. ومن ثم فان المشاركين في هجمات الارهاب الالكتروني يمكن اعتبارهم يخضعوا لهذا التوصيف القانوني.

١٣ – مبدأ الحياد في القانون الدولي

إن استخدام الفضاء الإلكتروني لشن هجمات يمثل انتهاكاً لمبدأ الحياد في القانون الولي حيث إن الفضاء الإلكتروني يمر عبر حدود العديد من الدول، ومن ثم فان الطابع الدولي للفضاء الالكتروني يجعل أياً من أطراف النظام الدولي معرضين للإصابة من جراء شن تلك الهجمات، كما انه إذا تم شن تلك الهجمات فإنها تمر عبر دولة ثالثة أو أكثر غير متورطة في الصراع وعلى الرغم من عدم مسئوليتها القانونية إلا أنها قد تصبح متورطة في تلك الهجمات، وهذا ما يعد انتهاكاً للقانون الدولي الإنساني

واتفاقية جينيف حيث جاء فيها " إن الدول والإطراف المشاركة في النزاع تمتنع عن تحريك القوات أو إرسال مستلزمات الحرب أو الإمدادات عن طريق أراضي الطرف المحايد ".

ويتحرك الفضاء الإلكتروني عبر شبكات الاتصال والمعلومات عابره للحدود وبالتالي فإنها تمر بدول محايدة، ويمكن أن تحمل أسلحة خاصة تختلف في التكتيك وطرق العمل ولكنها تدخل ضمن تعريف الأسلحة باعتبارها " أدوات للقتل أو إلحاق الضرر أو التسبب في وجود جرحي أو تدمير ممتلكات للخصم "، ومن ثم فان الدول المحايدة تمتنع عن نقل أسلحة الفضاء الإلكتروني عبر شبكات الاتصال والمعلومات التي تمر عبر أراضيها، فأسلحة الفضاء الإلكتروني يمكن أن تحدث الضرر بالمدنيين والمنشآت المدنية ولذلك فان هجوم الفضاء الإلكتروني مثل غيرة من أنواع الهجوم التقليدي، وقد يمر ذلك الهجوم عبر دولة أخرى وقد لا تشعر به .

<u>١٤- مبدأ مارتينز</u>

تم إدراج هذا الشرط في الفقرة ٢ من المادة الأولى من البروتوكول الإضافي الأول لعام ١٩٧٧ والذي ينص على أن" يظل المدنيون والمقاتلون في الحالات التي لا ينص عليها في هذا الملحق "البرتوكول أو أي اتفاق دولي أخر تحت حماية وسلطان مبادئ القانون الدولي كما استقر بها العرف ومبادئ الإنسانية وما يمليه الضمير العام " ويطلق هذا الشرط علية اسم المبدأ البديل باعتبار انه يطبق عند عدم وجود نص يحكم علاقة الشخص أو الأشخاص المعنيين بخصوص مسالة أو حالة لم يرد بشأنها نص صريح لذلك تقضي اتفاقيات جينيف على معالجة الحالات التي لم ينص عنها "على هدى المبادئ العامة الواردة في تلك الاتفاقيات في المادة ٤٥ و٤٦ من الاتفاق الأول والثاني.

<u>١٥- مبدأ إن المزايا الحربية لا يمكن أن تزيل حقوق الفئات المحمية</u>

حيث لا يجوز أن يترتب على الميزة العسكرية التي يرمي أي طرف من أطراف النزاع في تحقيقها إلى الاعتداء على الحقوق المقررة للفئات المحمية، إذ يجب إن يتم اتخاذ الاحتياطيات الواجبة لتجنب المدنيين والأشياء المدنية إلى أقصي قدر ممكن ويلات النزاع المسلح لذلك يحظر الهجمات العشوائية أو غير المميزة، ومثال ذلك الهجوم الذي يرتب آثاراً جانبية جسيمة على السكان المدنيين والأهداف المدنية بما لا يتناسب مع الفائدة العسكرية المتوقعة (م ٥١، ٥٢، ٥٧) من البروتوكول الإضافي الأول.

<u>١٦- حماية التراث الإنساني</u>

فقد نصت المادة ٥٣ من البرتوكول الإضافي الأول على حماية الأعيان الثقافية وأماكن العبادة ة في إطار أحكام اتفاقية لاهاي المتعلقة بحماية الأعيان الثقافية في حالة النزاع المسلح ١٤ مايو ١٩٥٤ والبروتوكول الثاني للاتفاقية المبرم في لاهاي في ٢٦ مارس1999، وأحكام المواثيق الدولية الأخرى الخاصة، فانه إذا ما طبقنا على الفضاء الإلكتروني فانه يحتوي على الأرشيفات الالكترونية الوطنية والثقافية والتاريخية للدول بما يشكل الحفاظ على الذاكرة الجمعية للدول والتراث الإنساني المشترك، ومن ثم فان هجمات الارهاب الالكتروني يمكن أن تخضع لهذه المادة .

## المطلب الثاني:
## مشروعية استخدام هجمات الإرهاب الالكتروني في حالة الدفاع الشرعي

أولا: الدفاع الشرعي ومحددات استخدامه في القانوني الدولي الإنساني:

يوجد في ميثاق الامم المتحدة قواعد قانونية تتعلق بحق الدفاع الشرعي كونه حق مشروع لكل معتدى عليه عندما يقع عليه فعل الاعتداء والذي يعدّ جريمة على النفس أو المال. ونظمت كل القوانين الداخلية نظمت وبيّنت نشوء هذا الحق واستعماله، و نصّت المادة (51) من ميثاق الأمم المتحدة على حق الدفاع الشرعي ونصت " ليس في هذا الميثاق ما يضعف أو ينقص الحق الطبيعي للدول فرادى أو جماعات في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء هذه الهيئة، وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين، وحتى عصبة الأمم المتحدة اعترفت بهذا الحق، و نصّ بروتوكول جنيف لعام ١٩٢٤ على هذا الحق في المادة 2 والتي جاء فيها أن الدول الموقعة قد اتفقت على أنها سوف لا تلجأ للحرب كوسيلة لفض النزاعات بأي حال إلاّ في حالة مقاومة العدوان.

ولاستعمال حق الدفاع الشرعي شروط في القانون الدولي حيث إن الرد يجب أن يتقيّد بشرطين: الأول -أن تكون القوة المبذولة للرد موجهة إلى مصدر الاعتداء فلا يجوز أن يكون المعتدي دولة وأن يوجه الرد لدولة أخرى وعندما تمارس هذه الحالة فإنها عدوان، والثاني -أن تكون القوة المبذولة للرد متناسبة مع العدوان. وفي حدود القدر الضروري لرد العدوان وإيقافه عند حده، وأجاز القانون الدولي فعل الدفاع الذي يمكن أن يمارس من الغير على مصدر الاعتداء شريطة أن يكون قرار التدخل حصراً لمجلس الأمن، وهذا ما نصّ عليه في مواد الميثاق ٣٩- ٤٠- ٤١- ٤٢ .[1]

وحددت المادة (٥١) الإطار المنظم لكيفية الدفاع الشرعي والذي يمكن إن يتم في شكل هجمات واضحة يتم تصنيفها كهجوم مسلح، وجاءت هجمات الإرهاب الإلكتروني أو حرب المعلومات لكي يتم شنها على نطاق واسع وأصبح انه ليس كافيا تصنيفها كهجوم مسلح وفق القانون الدولي التقليدي ومن ثم لا تخضع لسلطة قانون الاتفاقيات الدولية أو القانون الدولي العام أو القانون الجنائي العرفي.

كما إن ميثاق الأمم المتحدة يركز على مسالة تنظيم استخدام القوة فيما بين الدول وفق المادة ٢(٤) ووضعت شروط ونطاق التزام استخدام هذه القوة، وعند النظر إلي الهجمات التي يتم شنها في الفضاء الإلكتروني وفق ما جاء في نص المادة ٥١ فانه يبقى تساؤل حول إذا ما كان يمكن تصنيف تلك الهجمات باعتباره يخضع للتصنيف الخاص بالهجوم المسلح، ولكن عند التركيز على الوسائل المستخدمة في هجوم حرب المعلومات والإرهاب الالكتروني فانه يمكن القول أنها تضاهي ما يتم استخدامه في الحروب التقليدية في آثارها وتداعياتها كما ينتج من القنابل والأسلحة والقصف والعدوان وغيرها من مظاهر استخدام القوة داخل الفضاء الإلكتروني والذي يكون له نفس تأثير الهجمات

---

(1) نخبة من المتخصصين "القانون الدولي الإنساني،دليل التطبيق على الصعيد الوطني " تقديم، احمد فتحي سرور، دار المستقبل العربي، ٢٠٠٣ .

التقليدية [1]. وأكد ميثاق الأمم المتحدة على تحريم استخدام أو التهديد باستخدام القوة المسلحة ضد السلامة الإقليمية أو الاستقلال السياسي للدول الأعضاء في الأمم المتحدة وذلك مع وجود حالات الضرورة والتي حرص القانون الدولي على تحجيم ووضع قيود على الحرب إذا ما وقعت وأورد ميثاق الأمم المتحدة استثناءات لحالة الاستخدام المشروع للقوة في القانون الدولي وهي حالة الدفاع النفسي والجماعي الذي تضمنته المادة ٥١ من ميثاق الأمم المتحدة، والأخرى حالة حق تقرير المصير وحروب التحرير، وكذلك حالة العمليات الحربية التي يقوم بها المجتمع الدولي ، و التي يقرها مجلس الأمن التابع للأمم المتحدة وفق إحكام الفصل السابع.

وكل ذلك وفق الضوابط والشروط التي وضعها الميثاق لتنظيم القوة كما ورد في المادة ٢٠ ، ويفرض مجموعة من الشروط الموضوعية التي تتمثل في ضرورة وقوع عدوان مسلح بما يجعل استخدام القوة في إطار الدفاع الشرعي عن النفس أمرا مشروعا متفقا وصحيح القانون ومتناسبا ما بين العدوان وبين استخدام القوة دفاعا عن هذا العدوان، ومن ثم فان ذلك يستهدف الحد من استخدام القوة كعمل ثأري أو انتقامي يكون غير مشروع ومرتبا للمسئولية الدولية في حق من أقدم علية، أما الشروط الإجرائية أن تقوم الدولة التي تعرضت للعدوان بإبلاغ مجلس الأمن بوقوع العدوان وطبيعة ما اتخذته من إجراءات في مواجهته مع حقها في الدفاع عن نفسها ويتدخل مجلس الأمن ويباشر صلاحياته المخولة له حسبما تقضي به أحكام الميثاق.[2]

و أصبح المجتمع الدولي أمام نمط جديد من الحرب يحمل أساليب جديدة وهجوماً غير تقليدي في بيئة غير تقليدية ولها تداعيات غير محسوبة، وإذا ما نجحت فإنها تصيب المنشآت المدنية وتبث الرعب والخوف وتؤثر على الاستقرار السياسي داخل الدول وعلى المجتمع الدولي قاطبة، ففي احد السيناريوهات فان هجمات الإرهاب الالكتروني قد تتم من خلال الدخول إلى شبكات المعلومات بشكل غير شرعي، بما يؤثر على عمل البنية التحتية الكونية للمعلومات وما يكون له تأثير على الدول فرادي وعلى المجتمع الدولي ككل والذي أصبح يعتمد بشكل متزايد على تلك الشبكات الدولية لمسهلات لتقديم الخدمات التي تتعلق بنمط الحياة المعاصر.

والتي إن أصابها الضرر فإنها تهدد بوقوع خسائر وأضرار يقف خلفها دولة أو فاعل من غير الدول في مواجهه دولة أو أطراف من غير الدولة ، ويكون على اثر ذلك بروز عمليات دفاع شرعي تأتي في مضمونها مع الحق الذي أقرة القانون الدولي إلا إن ظروف استخدام هذا الحق وشروطه الموضوعة في ميثاق الأمم المتحدة أصبحت غير ملائمة لممارسة هذا الحق داخل بيئة جديدة وتحديات جديدة يفرضها استخدام القوة في الفضاء الإلكتروني للدفاع الشرعي ، كما يفرض تحديات تتعلق بإجراءات الوقاية والحماية ضد التعرض لمثل تلك الهجمات، ومن ثم فان أفعال الدفاع الشرعي قد لا تأتي في شكل القيام بهجوم مسلح تقليدي بل قد تتخذ أشكالاً أخرى وأن تأثيراتها وتداعياتها على الفضاء الإلكتروني

[1] Dimitrios Delibasis," State Use of Force in Cyberspace for Self-Defence:A New Challenge for a New Century" , Peace Conflict and Development: An Interdisciplinary Journal, Issue 8, February 2006,

[2] احمد عبد الونيس شتا " الدولة العاصية "، مرجع سابق ذكره ، ص ص ٢٠٠-٢٥٠

كمجال واحد يسبح به كافة المصالح والخدمات والتواصل العالمي ويشكل أهمية إستراتيجية للمجتمع الدولي، وينتج عن تعرضه لمسالة الدفاع والهجوم بلا شك تأثيراً على وظيفته وطبيعة دوره ومستقبله ويمس أهميته للمجتمع الدولي.

وثار جدل واسع حول طبيعة الأعمال الهجومية والدفاعية التي يمكن أن تحدث في الفضاء الإلكتروني، والذي أصبح يرتبط بالإستراتيجية العسكرية من خلال القدرة على شن طرق إنكار الخدمة أو الخداع أو التدمير أو الاستغلال، وهذا ما يفرض تحديات فيما يتعلق بمفهوم "العدوان" وهو الذي يعني استخدام القوة المسلحة من قبل دولة ضد السيادة أو الوحدة الإقليمية أو الاستقلال السياسي لدولة أخرى أو بأي طريقة أخرى لا تتفق مع ميثاق الأمم المتحدة، وليصبح العدوان جريمة بالمعنى القانوني الفعلي يجب أن يتوفر ويتحقق أركانها الأربعة وهي، الركن الشرعي والركن المادي والركن المعنوي والركن الدولي.

ويمكن أن تشن الدول العدوان من خلال الفضاء الإلكتروني أو مهاجمة نظم الاتصالات، أو قطع خدمة الإنترنت عن الدول الأعداء، أو استخدامه في الدعاية وشن الحرب النفسية والتجسس والقرصنة وتدمير قواعد البيانات الخاصة بمنشآت مدنية، وبما يقارب حالة القصف الجوي التقليدي، ولكن ذلك يتم عن طريق قصف فيروسات وهجمات داخل الفضاء الإلكتروني، أو التحريض على العنف داخل دولة معينة مستفيدة من الطابع الدولي للفضاء الالكتروني، ويقابل ذلك صعوبات في ما يتعلق بقدرة الدول على الوصول إلى مرتكب الهجوم عبر الفضاء الإلكتروني وانتهاك مفهوم السيادة للدول الأخرى، والقدرة على التمييز في حالة شن الهجمات وكيفية تحصين الدولة في مواجهه خطر التعرض لها.(1)

وأصبح العالم يواجه خطر تصاعد الهجمات عبر الفضاء الإلكتروني بالتزامن مع النمو ذاته فيما يتعلق بأسلحة الدمار الشامل، كما إن هناك دولاً عدة تعمل على نمو قدراتها في مجال حرب المعلومات وأسلحة الفضاء الالكتروني، وأخذت هجمات الكمبيوتر والفضاء الإلكتروني cyber attacks المزيد من الاهتمام إلى الحد الذي وضعته الدول في إطار إستراتجيتها العسكرية، وما يثيره ذلك من تساؤلات حول حدود استخدام القوة في الفضاء الإلكتروني للرد على الهجمات في إطار الدفاع الشرعي أو في استخدامها كنمط من استخدام القوة في العلاقات الدولية أو فيما يتعلق بالهجمات الوقائية حيث فرضت هواجس التعرض للخطر في إي وقت انتهاج شتى الطرق للحماية والتي تأخذ شكلا وقائيا أو استباقيا على مصدر التهديد المحتمل أو العمل على تقوية نظم الحماية والمنعة ضد التعرض لمثل تلك الهجمات.

ثانيا: محددات الدفاع الشرعي في حالة التعرض لهجمات الإرهاب الالكتروني:

إن قيام دولة بالهجوم على دولة أخرى يمكن إن يدفع الدولة المعتدي عليها القيام بهجمات دفاعاً عن النفس وتلك الهجمات لم يتم تحديدها قانونا في حق الدفاع الشرعي عن النفس، كما يواجه الهجوم في الفضاء الإلكتروني بتحديات تتعلق بخصائص هذا الهجوم الذي يتميز بان المهاجمين يتسببوا في سلسلة

(1) Dawn M. Gibson, " **Virtual Pandora's Box: Anticipatory Self-Defense in Cyberspace** ", uiowa univeresty , 2004,PP 201-341( http://www.uiowa.edu/~cyberlaw/csl03/dgcsl03.html#II)

من الإضرار عن طريق الدخول إلى نظم المعلومات، وتجعل طبيعة تلك الهجمات من الصعوبة تحديد مركز الهجوم المباشر بما يؤثر على فاعلية الرد الدفاعي. و لا توجد دولة يمكنها أن تصل إلى درجة عالية من المنعة ضد تلك الهجمات أما التحدي الثاني فيتعلق بإمكانية التعامل مع أي قاعدة قانونية جديدة تستطيع أن تنظم استخدام هجمات الإرهاب الإلكتروني في حالة الدفاع الشرعي عن النفس. فإذا ما تم استناد الدول إلى مثل ذلك في مواجهه هجمات الارهاب الالكتروني بصورة فردية فإنها تحمل وتتطلب تقدير لعدم مشروعيه العمل المبرر للرد، وتتطلب أن يتم التأكيد على أن تلك التدابير تلعب دورا أكثر فاعلية في العلاقات الدولية من أعمال الانتقام غير المبرر. وقد تنطوي تدابير الرد بالمثل على تعسف في استعمال الحق أو تمثل شكلا من أشكال التدخل في الشئون الداخلية للدولة التي حرصت علية مواثيق الأمم المتحدة على الحفاظ علية.

وتحمل هذه التدابير رداً على عمل غير مشروع دولياً، ومن ثم فإنها تلعب دورا هاما في إنقاذ القانون الدولي شانها في ذلك شان تدابير الانتقام، كما قد تعد نوعا من الجزاءات بالمعنى الفني الدقيق، وقد تكون تلك التدابير مؤقتة أو تنفيذية أو إكراهية أو عقابية بما يطرح مشكلة وضع نصوص تعمل على أن تقوم دولة بعمل إجراءات لحماية دولة أخرى في حالة التعرض لمثل تلك الهجمات حيث لا يوجد إطار قانوني يعاقب الدولة إذ ما امتنعت عن القيام بذلك.

وهناك تحدي أخر يتعلق بالحاجة إلى أن يتبنى المجتمع الدولي نظام قانون دولي يتعامل مع التنظيم الفعال لاستخدام هجمات الفضاء الإلكتروني وحرب المعلومات وأي أنشطة قد ترتبط بها والتمييز بينها، وتستطيع أن تتعامل مع أسلحة الكترونية حديثة وتكتيكاتها والتي قد تكون أدوات في أيدي فاعلين عدوانيين وكذلك إيجاد مفهوم واضح للهجوم المسلح، وهناك تحدياً أخر يتعلق بصعوبة التمييز بين هجمات شبكات الكمبيوتر التي ترتبط بالنشاط الإجرامي عن الأخرى التي ترتبط بأنماط الإرهاب عن النشاط الذي تقف وراءه وتسانده الدولة

وهناك عدداً من المفاهيم والتعريفات التي ترتبط بالحرب في الفضاء الإلكتروني ويمكن تفسيرها بطرق عديدة تبعا لمن يستخدمها والهدف من ورائها والذي يصعب تحديده بسهولة. أما القضية الأخرى التي يمكن أن تثار في إطار محاوله تنظيم هجمات شبكات الكمبيوتر والتي لم يتم تناولها في القواعد القانونية الخاصة بالدفاع الشرعي فهي أن الفضاء الإلكتروني يحمل بعدا عسكريا إلى جانب ما يحمل في الوقت نفسه بعدا مدنيا، وهذا ما يحتاج إلى تحديد مقتضيات وخصائص الهجوم الذي يعد عدوانا وحربا وإرهابا ومبدأ الدفاع الشرعي عن النفس بصفة خاصة وما يمكن إن يتعلق بالجهد الدفاعي أمام تلك الهجمات.

وتتطلب عملية دفاع وهجوم حرب المعلومات وهجمات الإرهاب الإلكتروني تعاونا بناء ما بين القطاع العام والقطاع الخاص والشركات العاملة في مجال من المعلومات وتكنولوجيا الاتصال والمعلومات داخل الدولة، حيث تتميز تكنولوجيا الاتصال والمعلومات بأنها من المجالات القليلة التي تحمل استخداما مزدوجا ما بين المدني والعسكري وهناك تحدياً يتعلق بإمكانية المواءمة ما بين الهجوم والرد علية وشرط التناسب مع فعل الاعتداء الذي هو شرط من شروط الدفاع الشرعي عن النفس وفق القانون

الدولي، حيث إن شبكات الكمبيوتر تسمح بتعدي آثار الاعتداء لأكثر من دولة، كما أن الرد على مثل هذا الاعتداء يتعدى أيضا أكثر من دولة دون القدرة على تحديد مصدر الهجمات، ومن ثم فإن الدفاع الشرعي يصبح عدوانا وذلك لعدم قدرته على التمييز، بالإضافة إلى إمكانية أحداثة أضراراً لا مبرر لها حيث يمكن أن تطول مرافق حيوية والتي فرض القانون الدولي حماية خاصة لها في أثناء النزاعات المسلحة.

ولا يوجد في مبدأ حظر استخدام القوة في العلاقات الدولية أي إلزام قانوني للدول داخل المجتمع الدولي للوقوف جانبا لمواجهه العدوان، ومن ثم فان القواعد القانونية التي تنظم استخدام القوة في حالة الدفاع الشرعي عن النفس ضد الهجمات لا توفر ضمانة للالتزام بها. كما لا توجد قواعد واضحة تحدد إن هناك دولة في حالة هجوم الكتروني وذلك تبعا للطبيعة الالكترونية والتكنولوجية التي يحدث بها فعل الاعتداء، حيث لا يستطيع من تعرض للهجوم أن يحدد تعرضه إلا بعد وقوع أثار فعلية تنتج عن هذا الاعتداء، حيث أن التعرض يكون فجائياً وهذا ما يكون له تأثيرات واضحة على الأمن والسلم الدوليين.

وقد أثارت محاولة تطبيق مبدأ الدفاع الشرعي على هجمات الفضاء الإلكتروني رؤى مختلفة حول مدى المواءمة القانونية وتطبيقاتها على تلك الهجمات خاصة وان ميثاق الأمم المتحدة لم يتناول على وجه التحديد مفهوم الضربات الوقائية للدفاع عن النفس، فوفقا إلى التفسير المتشدد فان حق الدفاع الشرعي عن النفس يتم فقط من جانب الدول للرد على هجوم مسلح. وهناك من يرى من الفقهاء أن ميثاق الأمم المتحدة لم يذكر ذلك صراحة، لاعتبار أن حق الدفاع الوقائي عن النفس يدخل ضمن العرف الدولي، ولكن يمكن استخدام الكمبيوتر كأداة من أدوات النزاع المسلح في حالة الدفاع الشرعي عن النفس فيمكن إن يعد استخدام هذا السلاح لصد عدوان مسلح يقوم على استخدام السلاح ذاته. ويصبح استخدام الفضاء الالكتروني كأداة من أدوات النزاع المسلح ولو كان في إطار الدفاع ولمواجهه عدوان مسلح بهذا النوع من الأسلحة يعد عملا غير مشروع لأنة إذا كانت الدولة المعتدي عليها تملك قانونا حق استخدام كل ما لديها من أسلحة وإمكانات عسكرية لدرء العدوان الواقع عليها ، فان هذا الاستخدام لكي يكون مشروعا يجب إن يكون متفقا والمبادئ الأساسية للقانون الدولي الإنساني باعتبارها مبادئ عرفية واجبة التطبيق في جميع الظروف والأحوال ومتماشية مع مبادئ قانون الحرب ، ومشروعية هجمات الارهاب الالكتروني .

و في السابق تم إثارة الجدل حول مدى اعتبار الأسلحة الكيماوية أو البيولوجية تعبيرا على استخدام القوة المسلحة وذلك على الرغم من أنها بمثابة وسيلة يمكن أن تتسبب في وقوع جرحى وقتلي مقارنة بالأسلحة التقليدية عن طريق استخدام الفيروس الحيوي أو الكيماوي، وعلى السياق نفسه فإن هجمات شبكة الكمبيوتر والإرهاب الالكتروني يتم فيها توظيف الإلكترون لكي يتسبب في التدمير أو الجرحى، وذلك دون أن يتم توصيف تلك الهجمات على أنها تعد "هجوما مسلحا".

وتكون هجمات الإرهاب الالكتروني جزءاً من عملية عسكرية شاملة في حالة النزاع المسلح، وإذا كانت تمثل هجوما وشيكا ويمكن أن تتسبب في أضراراً لا يمكن تجنبها ، ويمكن اعتبار هجمات

الإرهاب الالكتروني جزءا من النزاع المسلح إذا كانت مواكبة له أو أنها قد تكون منفصلة دون أن تكون هناك حاله عدائية ظاهرة، ويفرض ذلك إشكاليات التعامل مع المسئولية القانونية على تلك الهجمات. وتبقى مسالة خضوع هجمات الإرهاب الالكتروني للقانون الدولي على وجود عدد من المتطلبات، منها أنه يمكن اعتبارها استخداماً للقوة، إذا ما هدف ذلك الهجوم الدولي لإحداث الضرر المباشر لأهداف مدنية أو تسبب في جرحى أو هدد الوجود الإنساني، وانه في حالة عدم اعتبار هجمات الإرهاب الالكتروني جزءاً من استخدام القوة لكي يتم تطبيق ميثاق الأمم المتحدة عليها، فان طبيعة وخصائص وأثار الهجوم وطبيعته تدل على إنه استخدام للقوة.

و إذا ما كانت هجمات الكمبيوتر والإرهاب الالكتروني تعبيراً عن استخدام للقوة غير المسلحة أو غيرها فإنها تخضع للفصل السابع من ميثاق الأمم المتحدة ومبدأ الدفاع الشرعي عن النفس، و من ثم يمكن أن يتم الحكم بمدى مشروعية ذلك الهجوم إذا تم استخدام القوة بشكلها المسلح في الهجوم، ويمكن أن تخضع هجمات الإرهاب الالكتروني لنص المادة ٢(٤) وكذلك القانون الدولي العرفي والتي منعت جميعها استخدام القوة في العلاقات الدولية، وفي حالة استخدام القوة ليس فقط بشكلها المسلح ولكن تنطوي على ما من شأنه أن يحمل أي أعمال عدائية، وإذا لم ترق هجمات الإرهاب الالكتروني لمستوى استخدام القوة فانه يمكن النظر إليها باعتبارها تعد تدخلا في الشئون الداخلية للدول الأخرى وهو ما يحرمه الميثاق.

وفي حالة استخدام تلك القوة من قبل الدول عن طريق الهجوم باستخدام شبكات الكمبيوتر، وإن مجلس الأمن يمكنه أن يصف ذلك على انه عمل من أعمال العدوان أو يمثل تهديداً للسلم الدولي، و يمكن إخضاعه لنص المادة ٤٢ من الميثاق وفي حالة إذا لم تأت هجمات شبكات الكمبيوتر في شكل هجوم مسلح فان مجلس الأمن قد يرى فيها تهديدا للسلم الدولي بما يخوله من حق استخدام القوة لمنع تهديد السلم الدولي. والدول سواء أكانت بشكل فردى أو مجموعات قد تستخدم هجمات الفضاء الإلكتروني بشكلها المسلح للدفاع الشرعي وفق المادة ٥١ من الميثاق، كما إن الدول قد تستجيب بشكل فردي أو جماعي إلى التهديد باستخدام تلك الهجمات غير ذات الطابع المسلح ليس برد فعل عسكري بالضرورة .

وقد يأتي رد الفعل الشرعي في شكل إجراءات حماية أو تعاون امني مشترك، ومن ثم فان مسالة الدفاع الشرعي قد تتضمن جزأين الأول يتم من خلال دعم البنية التحتية للمعلومات وتامين الفضاء الإلكتروني ودعم التعاون الدولي، أما الثاني فهو يأتي بعد التعرض للهجمات أو في أثنائها أي أن الدفاع قد يكون عبارة عن رد فعل أو له طابع وقائي. ويمكن أن تعد مسألة استخدام أسلحة الفضاء الإلكتروني بكل أنواعها تخالف في حالة استخدامها مبدأ التناسب وهو أحد المبادئ الجوهرية التي تكون واجبة التطبيق في حالة النزاعات المسلحة بكافة أنواعها الدولية والداخلية، ويرمي هذا المبدأ إلى الإقلال من الخسائر أو أوجه المعاناة المترتبة على العمليات العسكرية سواء بالنسبة للأشخاص أو الأشياء، ومن ثم فإذا كانت وسائل القتال المستخدمة لا يوجد تناسب بينها وبين الميزة العسكرية

المرجوة من العملية العسكرية فلا يجوز استخدامها.[1] ويعد القيام بشن هجمات ضد البنية التحتية الكونية للمعلومات امتدادا تلقائيا لاستخدام القوة في العلاقات الدولية، ووفق هذا التحليل فإن الدول قد تلجأ للرد على هذا الهجوم ليس فقط في إطار الرد التناسبي للدفاع الشرعي، ولكن أيضا قد يأخذ شكل الضربات الوقائية للدفاع الشرعي ، حتى إذا لم يتم اعتبار هجمات الفضاء الإلكتروني ضمن تعريف ميثاق الأمم المتحدة للهجوم المسلح في المادة ٥١ ويعني ذلك اتساع استخدام حق الدفاع الشرعي بما يدخل ضمن الإعمال العدائية التي يجرمها القانون الدولي حيث يقر القانون الدولي بعده ضوابط لاستخدام حق الدفاع الشرعي، والذي يستلزم الوقوع تحت خطر" الهجوم الوشيك ".

وسيؤدي ذلك إلى اتساع استخدام القوة تحت ذريعة الدفاع الشرعي، كما إن الأخطار غير العسكرية يمكن إن ترتفع بدرجة التهديد لمستوى الهجوم المسلح والذي "يصبح له تداعيات دولية من خلال انتهاك السيادة الإقليمية لدولة أخرى، كما أن أخطار الأعمال غير ذات الطابع العسكري التي يمكن استخدامها من قبل الدول من الممكن أن تعد أو تصل إلى مستوى الهجوم المسلح، وذلك عندما تتسبب في هجوم ذي طابع دولي يؤدي إلى اثر تدميري في دولة أخرى ذات سيادة. وأصبحت تتطلب تلك الصراعات غير تقليدية استجابات غير تقليدية.

ويمكن أن تأتي عملية الهجوم من خلال الفضاء الإلكتروني كجزء من حرب مستقلة أو جزء متواكب مع الحرب التقليدية أو إن تقوم بها جماعات إرهابية ضد دول معينة أو يقوم بها قراصنة والواضح أنة لم يتوصل المجتمع الدولي إلى تقنين واضح وصريح بشان الموقف من استخدام حرب المعلومات والإرهاب الالكتروني أو التهديد بها سواء وقت السلم أو الحرب، وبناء علية فان ما يمكن الارتكاز علية هو تعارض تلك الحرب مع ما استقر علية العرف والقوانين الدولية ومنها القانون الدولي الإنساني، وجدير بالذكر إن هناك جهود مضنية دارت حول فكرة التجريم الدولي لأسلحة الدمار الشامل وفق مبدأ حظر التهديد باستخدام القوة في العلاقات الدولية وفق ميثاق الأمم المتحدة.

و يبرز دور المحكمة الجنائية الدولية ومحكمة العدل الدولية في تولى مهمة وضع تشريع دولي يحرم استخدام الحرب المعلوماتية ضد الأماكن الحيوية أو يقنن استخدامها أو التهديد بها وفق قانون الحرب واستقر العمل الدولي على التزام المقاتل في الحرب بصفة عامة بعدم استعمال الأسلحة أو المواد المحرمة أثناء العمليات الحربية لما ينطوي عليه ذلك من تجاوز للحدود التي يرسمها قانون الحرب والذي يستمد مصادرة من الاتفاقيات الدولية العديدة، والذي اقر بأن حق المتحاربين ليس مطلقا في اختيار وسائل الإضرار ببعضهم [2]،ولما يمكن أن تسببه من أضرار للمدنيين وعدم التمييز بين المقاتلين وغير المقاتلين، وإمكانية إصابة منشآت حيوية تتعلق بالبنية التحتية الكونية، خاصة فيما يتعلق بعدم إمكانية التحكم في حجم الضرر وعلاقته بأمن المجتمع الدولي.[3] وأقر ميثاق الأمم المتحدة في المادة ٢

---

(1) كما ورد في المادتين ٥١، ٥٧ من البرتوكول الإضافي الأول العام ١٩٧٧ .

(2) إبراهيم محمد العناني "المحكمة الجنائية الدولية ومنع انتشار أسلحة الدمار الشامل، الفصل الثالث في " اعمل الندوة الفكرية "الخيار النووي في الشرق الأوسط، مركز دراسات المستقبل جامعه أسيوط ٢٠٠٢، ص ص ١٠٣-١١٩ .

(3) د.احمد عبد الو نيس شتا "القانون الدولي والأسلحة النووية " ،بحث غير منشور ، ندوة "إخلاء منطقة الشرق الأوسط من أسلحة الدمار الشامل :الجوانب القانونية ،منتدى القانون الدولي ، كلية الاقتصاد والعلوم السياسية ، جامعه القاهرة ، ١٩ /٤ / ٢٠٠٤ .

في الفقرة ٤ "بأن يمتنع أعضاء الهيئة جميعا في علاقاتهم القوة، عن التهديد باستعمال القوة واستخدامها ضد سلامة أراضي أو الاستقلال السياسي لأية دولة أو على أي وجه أخر لا يتفق ومقاصد الأمم المتحدة "وتؤكد طبيعة الالتزام بتقييد استخدام القوة بأنة ذا طابع سلبي بحيث تمتنع الدول عن اللجوء إلى القوة، ويعد نطاق الالتزام بعدم استخدام القوة التزام شامل.

كما إن استخدام هجمات الإرهاب الالكتروني قد تدخل ضمن أعمال الانتقام العسكرية، والتي لا تتفق مع روح الميثاق ويتعارض صراحة مع الإعلان الصادر عن الجمعية العامة للأمم المتحدة بخصوص المبادئ التي تحكم العلاقات الودية بين الدول لعام ١٩٧٠، والذي ينص صراحة على واجب الدول في الامتناع عن أعمال الانتقام العسكرية ويعد الإرهاب الالكتروني في ظل تلك المادة نوعا من العدوان غير المباشر وما يمكن أن يرتب من مسئولية دولية عن تلك الأفعال، التي تعده الدولة المعتدى عليها عدواناً من دولة أخرى، وبما قد يؤدى إلى احتدام حدة الصراع بشكله التقليدي وغير التقليدي، و بما يشبه حالة الفوضى التي تمتد آثارها إلى العالم أجمع الذي يرتبط بالبنية التحتية الكونية للمعلومات، ومع وجود فاعلين من غير الدول وعدم وضوح الجهة المعتدية.

وتدفع عدم واقعية المبدأ الخاص بتناسب الرد في حالة الدفاع الشرعي باستخدام هجمات الفضاء الالكتروني إلى صعوبة القياس أو التحكم في تلك الهجمات، وكذلك عدم التحقق من مبدأ الملاءمة من الناحية القانونية ويأتي هالثالث: المادة ٤١ التي تقرر بأن" لمجلس الأمن أن يقرر ما يجب اتخاذه من التدابير التي لا تتطلب استخدام القوات المسلحة لتنفيذ قراراته، وله أن يطلب إلى أعضاء "الأمم المتحدة" تطبيق هذه التدابير، ويجوز أن يكون من بينها وقف الصلات الاقتصادية والمواصلات الحديدية والبحرية والجوية والبريدية والبرقية واللاسلكية وغيرها من وسائل المواصلات وقفا جزئياً أو كليا وقطع العلاقات الدبلوماسية."[1]

ويمكن أن يتسبب استخدام هجمات الفضاء الإلكتروني في حالة الدفاع الشرعي في تدمير مباشر وغير مباشر أو إحداث ضرر بالمدنين غير مبرر بما يشكل صعوبة تنفيذ أو استخدام حق الدفاع الشرعي عن النفس، وبما يتعارض مع نص المادة ٥١ والتي تقضي بأنه "ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس - بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق - من الحق في أن يتخذ في أي وقت ما يراه ضرورياً لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه ويمكن لهجمات شبكات الاتصال المعلومات بواسطة شن هجمات الإرهاب الالكتروني أن تشر الدمار وتتسبب في وقوع خسائر اقتصادية وإضراراً بالحياة المدنية، والتي يمكن أن تدخل ضمن أعمال مجلس الأمن واختصاصه باعتباره هيئة دولية تختص بالسلم والأمن الدوليين.

---

(1) المادة ٤١، الفصل السابع من ميثاق الأمم المتحدة

## المطلب الثالث:

## موقف الشريعة الإسلامية و محكمه العدل الدولية و المحكمة الجنائية الدولية

أولا : الشريعة الإسلامية كمصدر من مصادر التشريع الدولي

كانت الشريعة الإسلامية اسبق من القانون الدولي في وضع قواعد للحرب والقتال بل وتحريم الاقتتال في أربعه اشهر من السنة وتم إرساء قواعد شكل قاعدتها الأساسية آيات القران الكريم والسنه النبوية التي لا تحض على العدوان وان الحرب هي للدفاع عن النفس ففي وصية الرسول (ص) لقادة الجيش في كافة الغزوات قال (انطلقوا باسم الله وعلى بركة رسوله لا تقتلوا شيخًا ولا طفلاً ولا صغيرًا ولا امرأة ولا تغلوا "أي لا تخونوا"، وأصلحوا وأحسنوا إن الله يحب المحسنين)، كما نهى صلى الله عليه وسلم عن المثله أي التمثيل بالجثث فقال: (إياكم والمثله ولو بالكلب العقور)، وقال أيضًا: (لا تقتلوا ذرية ولا عسيفًا، ولا تقتلوا أصحاب الصوامع).[1]

وفقا للتعريف الفقهي لمفهوم الجهاد ينقسم إلى جهاد اكبر وجهاد اصغر، ويتعلق الجهاد الأصغر بالقتال المشروع لمواجهه العدوان ،أما الأصغر هو مجاهدة النفس لجلبها على السمو الأخلاقي ، ومن ثم فان ما يستخدم من هجمات ضد مواقع مدنية ذات مرافق حيوية بدون وجود مبرر للعدوان أو لبث الخوف فهو نوع من الإرهاب أما إذا دخلت في مجال حرب المعلومات ضد من يعلن عداءة فهي نوعا من الجهاد والتي تختلط مع مقاومة العدوان . وقد أيد الشيخ القرضاوي الجهاد الالكتروني معتبرا إن «كل هذه أعمال عظيمة والمقاومة يجب أن تلجأ لكل الوسائل المتاحة»[2] ووجهة نظر الإسلام في هذه القضية واضحة، حيث إن هذه العملية هي بمثابة سرقة - وإن لم تكن حسية- لشيء لا تملكه، بل يعتبر من خصوصيات الشخص، والله عز وجل نهانا عن التجسس، قال تعالى: "ولا تجسسوا ولا يغتب بعضكم بعضا .وأما تدمير المواقع المعادية للمسلمين وتلك التي تنشر أفكارا هدامة، فقد أشارت بعض الفتاوى أن لا محصلة للمسلمين في ذلك؛ لأنّ هذا قد يكون مدعاة لمهاجمة مواقعنا الإسلامية.

وترتكز تلك الفتاوى بالأساس على قوله تعالى" ولا تسبوا الذين يدعون من دون الله فيسبوا الله عدوا بغير علم كذلك زينا لكل أمة عملهم ثم إلى ربهم مرجعهم فينبئهم بما كانوا يعملون"(الأنعام ١٠٨ )غير أن هناك بعض الفتاوى الشرعية ترى أنه لو بدأ الأعداء بتدمير مواقع الإسلام على الإنترنت، فمن حقّنا أن نردّ عليهم بالمثل امتثالا لقوله تعالى:{وجزاء سيّئة سيّئة مثلها}. بل من واجبنا في هذه الحالة أن نقوم بتحطيم مواقعهم المعادية للإسلام؛ لأنّ ذلك هو الوسيلة الوحيدة لردعهم عن تحطيم مواقعنا الإسلامية، وهذا أمر حصل فعلا فيما عرف بظاهرة "الجهاد الإلكتروني" عن طريق اختراق بعض المواقع العنصرية التي تهاجم الإسلام وتحث على تدمير المواقع التي تسعى لنشر الدعوة إلى الله في أرجاء المعمورة.

---

(1) للمزيد انظر المستشار/ علي علي منصور، الشريعة الإسلامية والقانون الدولي العام، المجلس الأعلى للشئون الإسلامية، ١٩٦٥م، ص ٢٤١. وأيضا ، د. السيد مصطفي احمد أبو الخير،" نظرية الحرب في الإسلام" موسوعة الإعجاز العلمي في القران والسنة (http://www.55a.net/firas/arabic/?page=show_det&id=1034&select_page=8) (٣-١-٢٠٠٩)

(2) القرضاوي يؤيد الجهاد الإلكتروني ضد إسرائيل، الجزيرة نت ، ١-٩-٢٠٠١.
(http://www.aljazeera.net/News/archive/archive?ArchiveId=15352،)

وتبقى الإشارة إلى ضرورة التزام بني البشر من سائر الأديان والأجناس بعدم استغلال الإنترنت لنوايا شريرة، وأن يكون هناك ميثاق شرف يمتنعون به عن تهديد المواقع لأن ذلك لن يجدي فتيلا، فالإنترنت فضاء مفتوح يتيح لسائر الناس أن يختاروا ما يحلو لهم من مواقع وخدمات، وهو الذي يتيح للمسلمين فرصا كبيرة لجعل صوت الإسلام مسموعاً في كلّ بلاد الدنيا، ولا شك أن إنشاء المواقع للعدوان وتضليل الآخرين ونشر الأفكار الهدامة لا يجوز .

ولقي الجهاد الإلكتروني ترحيبا من قبل لجنة الفتوى بالأزهر الشريف التي أفتت بجواز استخدام التكنولوجيا الحديثة في الهجوم على المواقع الإسرائيلية والأمريكية والمواقع التي تسيء للإسلام والمسلمين وتدميرها، وكذلك الرد عليها؛ باعتبار أن ذلك نوع من أنواع الجهاد المعاصر، ويقول سماحة مفتي عام المملكة الشيخ عبد العزيز بن عبد الله آل الشيخ : (شبكة الإنترنت من وسائل الاتصالات الحديثة السريعة في إيصال المعلومات الواسعة من حيث الانتشار وسهولة الوصول إليها وهي إن استغلت في الخير والدعوة إلى الله ونشر دين الله في أصقاع الأرض من قبل الأفراد والمؤسسات الإسلامية المختلفة ، فلا شك أنها من الجهاد في سبيل الله بالبيان واللسان ويجب على المسلمين استغلالها وتسخيرها لهذا الغرض الخير ، أما المواقع الفاسدة المخلة والمضرة بعقائد المسلمين من خلال التلبيس والتشكيك والمضرة بأخلاقهم كذلك من خلال ما يعرض فيها من الدعوة إلى الفساد وتيسير طرقه وتعليم الناشئة لهذه الأمور ، وتربيتهم عليها من خلال ما يعرض فيها ... فلا ريب أن هذا من أعظم المنكرات التي يجب التصدي لها وإنكارها وفق قواعد إنكار المنكر التي جاء بها النص من الكتاب والسنة ، وبينها وفصلها علماء الأمة" [1].

<u>ثانيا: موقف محكمة العدل الدولية من استخدام أسلحة الفضاء الالكتروني والقياس على الأسلحة النووية</u>

قدمت الجمعية العامة للأمم المتحدة في عام ١٩٩٤ طلبا لمحكمة العدل الدولية حول إبداء رأيها الاستشاري حول مشروعية استخدام الأسلحة النووية، وجاء رأيها أن التهديد أو استخدام الأسلحة النووية يتعارض بشكل عام مع قواعد القانون الدولي التي تتعلق بحالة النزاعات المسلحة، وبالتحديد قواعد القانون الدولي الإنساني، ولكن بالنظر إلى الوضع الحالي للقانون الدولي فان " محكمة العدل الدولية تذهب إلى القول بان مبادئ وقواعد القانون الذي يتناول الصراع المسلح وبالنظر إلى روح وقلب مبادئ الإنسانية التي تجعل من الأعمال المسلحة خاضعة لعدد من المطالب والشروط لذلك فان وسائل وطرق الحرب التي ربما تعمل على إزالة التمييز مابين المدنيين وغير المدنيين والأهداف المدنية والعسكرية أو النظر إلي ما قد يترتب علي استخدامها من آلام أو أضرار لا مبرر لها للمحاربين تصبح محرمة " [٢].

---

(1) للمزيد حول موقف الشريعة الإسلامية من القانون الدولي الإنساني انظر : احمد ابو الوفا ، النظرية العامة للقانون الدولي الإنساني في القانون الدولي وفي الشريعة الإسلامية ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠٠٦ ص ص ١٦٥-٢١٥،

(2) تعد محكمة العدل الدولية منظمة منبثقة عن الأمم المتحدة وأنشئت بموجب ميثاقها في عام ١٩٤٥ وبدأت عمليها في ابريل عام ١٩٤٦ ويوجد مقرها في لاهاي ، وللمزيد حول رأيها الاستشاري حول استخدام السلاح النووي في النزاع المسلح في عام ١٩٩٤ انظر موقعها على الإنترنت www.icj-cij.org وكذلك الاطلاع على : Legality of the Use by a State of Nuclear

وبالنظر إلى خصائص السلاح النووي غير التقليدية وآثارها والتي تجعل من استخدام هذه الأسلحة في الواقع تبدو كارثية بما يدعو إلى إن يتم التعامل معها وفقا لتلك الاعتبارات القانونية التي يتم التعامل بها في مثل تلك الحالات وفق القانون الدولي بما يخضع السلاح النووي لقواعد النسبية والضرورة والوسطية والتمييز والحياد والإنسانية وحماية المدنيين (1)".

ويمكن ملاحظة عده أمور أهمها ما يتعلق، أولا بموقف القانون الدولي من أسلحة حديثة لم تتم الإشارة إليها في قانون الحرب بالتجريم أو بشكل محدد، وثانيا انه تم التوافق ما بين طبيعة تلك الأسلحة والمبادئ العامة التي كان من شانها تجريم استخدامها الأسلحة الأخرى بموجب القانون الدولي، وثالثا، يعد ذلك سابقة تاريخية تدخل في إطار العرف الدولي ويمكن إن يتم تطبيقها على أي أسلحة يكون من شانها إحداث ذلك الضرر أو الأثر بالمجتمع الدولي يخالف قواعده العامة.

ويمكن لبعض التأثير الذي يتعلق بالأسلحة النووية أن يتشابه مع حالة الهجوم عن طريق استخدام أسلحة وهجمات الفضاء الإلكتروني، ويتم في مثل هذه الهجمات التعرض لكل البنية التحتية الكونية للمعلومات لخطر الدمار والتعطيل، بما يكون له من اثر على الدولة التي تكون ضحية لتلك الاعتداء وأيضا ما يتصل بتهديد المجتمع الدولي ككل عن طريق شبكات الاتصال والمعلومات التي تربط دول العالم بعضها ببعض وتزايد درجات الاعتماد المتبادل بين دول العالم، وما ينتج عن ذلك من انتهاك لقيم ومبادئ القانون الدولي الذي عمل على إرساء الاستخدام السلمي والتعاون والتفاهم بين شعوب العالم.

وقد كان الهجوم على استونيا ابريل ٢٠٠٧ وكذلك استخدام هجمات الفضاء الإلكتروني في الحرب الجورجية الروسية أغسطس ٢٠٠٨ بالإضافة إلى الاستخدام غير السلمي للفضاء الالكتروني من قبل الجماعات الإرهابية أو جماعات الجريمة المنظمة والقراصنة وغيرها بما يمثل انتهاكا للطابع السلمي للفضاء الالكتروني عن طريق استخدام أسلحة الفضاء الإلكتروني التي تتميز بالتنوع ما بين هجمات الفيروسات وإنكار الخدمة أو سرقة المعلومات أو إفساد أو تعطيل النظم المعلوماتية أو بث الشائعات أو المعلومات المضللة، ويمكن أن توجه تلك الأسلحة إلى دولة معينة أو مؤسسات محددة ولكن يكون لها تأثير كبير على المجتمع الدولي عبر شبكات الاتصال والمعلومات والتي تتمدد في الدول النامية والمتقدمة على السواء.

وقد يتم تطوير تلك الأسلحة بدون أي تكاليف مادية باهظة، وهناك توافر لمصادر المعرفة الكاملة عنها عن طريق ما يتم تداوله عبر مواقع الإنترنت حيث يتم إتاحة معلومات عن القراصنة والاختراق وسرقة المعلومات وفك التشفير وضرب البرامج وغيرها ويمكن لأي فرد أن يتعلمها سواء بدافع ذاتي أو عن طريق توظيفه من قبل جماعات إرهابية أو جريمة منظمة أو أن تستخدمه الدول، وهذا ما يظهر في انتشار تلك الأسلحة أو نقلها واستخدامها وتخزينها وعدم خضوعها للرقابة مقارنة بحال الأسلحة النووية

---

Weapons, in Armed Conflict, Advisory Opinion, I. C. J. Reports 1996, p. 66, Nuclear Weapons Advisory Opinion 95, at 32, 35 I.L.M. at 829.

(1) **On the Unlawfulness of the Use and Threat of Nuclear Weapons**, Report of the Foreign and International Law Committee of the New York County Lawyers' Association, available at: http://www.nuclearweaponslaw.com/JournalsReport/NYCLA_Report.pdf. Last visited: Feb. 24, 2008

[1]. وهذا ما يدخل عملية استخدام تلك الأسلحة عبر الفضاء الإلكتروني ضمن الهجمات المتعمدة والعشوائية وغير المتناسبة التي تسبب الأضرار للمدنيين، فهي لدى ارتكابها بقصد إجرامي، تعتبر جرائم حرب. ويمكن أن يصبح الأشخاص القائمين عليها عرضة أيضاً للمسؤولية الجنائية في إطار ارتكاب جريمة حرب، وكذلك ما يتعلق بالمعاونة فيها أو تسهيلها أو المساعدة على ارتكابها أو الحث عليها. [2]

وترجع أهمية القياس على الأسلحة النووية لأنه لا يوجد موقف دولي واضح من هجمات الفضاء الإلكتروني ولا توجد سوابق قانونية يمكن الاستناد إليها، وهذا ما يدفع إلى ضرورة الوصول إلى نظم قانونية يمكن إن تنشئ قواعد خاصة بتنظيم استخدام الفضاء الإلكتروني وتجريم استخدامه في الأغراض العسكرية، أو تلك الأنشطة التي تضر بأهميته ودورة في المجتمع الدولي وهذا ما يتطلب أهمية الوصول إلى اتفاقية دولية شاملة حول الأمن الالكتروني. ويمكن أن تتم معاملة الأسلحة الالكترونية وما قد ينتج عن استخدامها في حالة الدفاع الشرعي أو في النزاع المسلح في إطار الأضرار الجسيمة التي تلحق بالمجتمع الدولي، وكيف يمكن الاستفادة من الجهود الدولية من تجريم استخدام الأسلحة النووية.

وفي الرأي الاستشاري لمحكمة العدل الدولية حول مشروعية استخدام الأسلحة النووية وجدت أن "... القوة التدميرية للأسلحة النووية لا يمكن منعها سواء من حيث المدى أو الزمن... ستؤثر الطاقة الإشعاعية المنطلقة من الانفجار النووي على الصحة، والزراعة، والموارد الطبيعة وجغرافيا على نطاق واسع للغاية وبالإضافة إلى ذلك، يشكل استخدام الأسلحة النووية خطراً جسيماً على الأجيال القادمة..." وذهبت محكمة العدل الدولية في رأيها الاستشاري يوليو ١٩٩٦ في نفس الاتجاه حين أقرت بوجود التزام على الدول النووية بمواصلة المفاوضات بحسن نية للتوصل إلى نزع السلاح النووي بكل أشكاله تحت رقابة دولية صارمة و فعالة.

ويشكل القرار الخاص بمبادئ و أهداف عدم الانتشار و نزع السلاح النووي في فقرته ٤/ج وكذا الالتزامات التي قطعتها الدول النووية على نفسها خلال مؤتمر المراجعة السادس لسنة ٢٠٠٠ الذي التزمت خلاله بصفة قطعية بإزالة أسلحتها النووية بالكامل في اتجاه نزع السلاح النووي الكامل لاسيما الخطوات العملية ١٣ التزامات قائمة في إطار إعمال المادة ٦ من معاهدة عدم الانتشار.

---

[1] وبلغ ذلك إلى حد تشبيه أسلحة الفضاء الإلكتروني بأسلحة الانتشار الشامل على نسق أسلحة الدمار الشامل حيث انتشار وإتاحة إمكانية امتلاكها واستخدامها ونقلها وتطويرها بدون تكلفة كبيرة بما يمكن أن يتيح ذلك للدول الصغرى والجماعات الإرهابية والأفراد من تطويرها واستخدامها كوسيلة لتحقيق أغراض سياسية أو إجرامية أو غيرها .

[2] N. C. Rowe, War Crimes from Cyber-weapons.Journal of Information Warfare,No 6, December 2007,pp15-25

ثالثا : هجمات وأسلحة الإرهاب الالكتروني وموقف المحكمة الجنائية الدولية[1] كشكل من أشكال العدوان:

أنشئت المحكمة الجنائية الدولية في عام ٢٠٠٢ ويمكن أن تخضع هجمات الارهاب الالكتروني لاختصاص هذه المحكمة فيما اعتبرته المحكمة جرائم إبادة جماعية، والتي تعني أي فعل يرتكب بقصد إهلاك جماعه أو إلحاق ضرر جسدي أو إخضاعه عمدا لأحوال معيشة مزرية، وهذا ما قد ينتج إذا ما تعرضت دولة ما أو مجتمع إلى الحرمان من الحصول على الخدمات أو تدمير البنية التحتية للمعلومات مما يؤدي إلى إضرار اقتصادية جسيمة من جراء التعرض لهجمات الفضاء الإلكتروني، إما عن توصيف جرائم ضد الإنسانية والتي تعني أي هجوم أو فعل يرتكب ضمن إطار هجوم واسع النطاق موجه ضد أية مجموعة من السكان المدنيين. ويظهر ذلك في حالة شن هجمات الفضاء الإلكتروني التي تتميز بالانتشار الواسع عبر شبكات الاتصال والمعلومات والحرمان من الحرية للأفراد.

أما عن اعتبار هجمات الفضاء الإلكتروني تقع ضمن مجموعه جرائم الحرب حيث أنها تمثل إذا ما تم القيام بها انتهاكا لاتفاقيات جينيف وما تتضمنيه من حظر القيام بالتسبب في معاناة شديدة أو إصابات خطيرة بالجسم أو الصحة، أو تدمير الممتلكات والاستيلاء عليها، أو توجيه هجمات ضد السكان والمنشآت المدنية التي ترتبط في عملها بالفضاء الإلكتروني. ومن ثم فان المسئولين عن تلك الهجمات يمكن اتهامهم بارتكاب جرائم حرب[2] كما تعد هجمات الفضاء الإلكتروني نوعا من العدوان على الرغم من عدم الاتفاق حول تعريف واضح له إلا انه وفق قرار الجمعية العامة للأمم المتحدة في ١٤ ديسمبر ١٩٧٤ اقر بان العدوان هو "استعمال دولة ما، القوة المسلحة ضد دولة أخرى ضد السيادة وسلامة الأرض والحرية السياسية أو بأية طريقة أخرى". ، وبالقياس على استخدام أسلحة الفضاء الإلكتروني نجد أنها تمثل نوعا من استخدام القوة ذات الطابع المرن أو الالكتروني التي ينتج عن استخدامها غير مشروع نفس نتائج استخدام القوة بمفهومها التقليدي.

---

(1) وهي منظمة دولية دائمة، تسعى إلى وضع حد للثقافة العالمية المتمثلة في الإفلات من العقوبة – وهي ثقافة قد يكون فيها تقديم شخص ما إلى العدالة لقتله شخصا واحدا أسهل من تقديمه لها لقتله مائه ألف شخص مثلا، فالمحكمة الجنائية الدولية هي أول هيئة قضائية دولية تحظى بولاية عالمية، وبزمن غير محدد، لمحاكمة مجرمي الحرب ومرتكبي الفظائع بحق الإنسانية وجرائم إبادة الجنس البشري. ، و بلغ عدد الدول الموقعة على قانون إنشاء المحكمة ١٠٥ دول حتى تشرين الثاني نوفمبر ٢٠٠٧، وقد وقعت ٤١ دولة أخرى على قانون روما لكنها لم تصادق عليه بعد، وقد تعرضت المحكمة لانتقادات من عدد من الدول منها الصين والهند وأمريكا وروسيا، وهي من الدول التي تمتنع عن التوقيع على ميثاق المحكمة.و تعد المحكمة الجنائية هيئة مستقلة عن الأمم المتحدة، من حيث الموظفين والتمويل، وقد تم وضع اتفاق بين المنظمتين يحكم طريقة تعاطيهما مع بعضهما من الناحية القانونية.

(2) **Jefferson D. Reynolds, Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground, 56 A.F. L. REV. 1 ,2005**

## المبحث الثالث:

## الفضاء الالكتروني

## وفق قانون الفضاء الخارجي وقانون البحار.

**يحاول الباحث في هذا المبحث الاستفادة مما استقرت عليه القواعد والأطر القانونية التي أصبحت ترقى إلى منزلة العرف الدولي والتي كان لها الدور في ترسيخ قيم إنسانية مشتركة تعزز الاستخدام السلمي والتعاون المشترك وكان لاتفاقية الفضاء الخارجي والأجرام السماوية لعام ١٩٦٧ والاتفاقية الدولية للبحار لعام ١٩٨٢ الدور في ذلك ويتم تأكيد ذلك عبر تناول الباحث في المطلب الأول:التكييف القانوني للإرهاب الالكتروني في ظل قانون الفضاء الخارجي ، ويتم تناول في المطلب الثاني: التكييف القانوني للإرهاب الالكتروني في ظل القانون الدولي للبحار.**

### المطلب الأول:

### التكييف القانوني للفضاء الالكتروني

### وفق اتفاقية الفضاء الخارجي والأجرام السماوية

يتشابه الفضاء الإلكتروني مع الفضاء الخارجي والى حد بعيد أعالي البحار وأيضا القارة القطبية فيما يعرف بنظرية الفضاءات الدولية، حيث توجد مساحات حرة ومتنوعة تمارس فيها الدول أنشطة الاستخدام دون اعتراض من جانب الدول الأخرى ما دامت هذه الممارسة تقع في حدود مقبولة ويحسب مقتضيات الاستخدام والاستغلال السلمي، وهناك اتفاق عام على إن مصالح المجتمع الدولي تتعارض والاعتراف لأية دولة بسيادتها على هذه المناطق، ويتعارض الاعتراف بحق دولة في السيطرة والتحكم في الفضاء الإلكتروني مع مصالح الدول جميعا، وإن استخدام الفضاء الكتروني في أغراض تتنافى ومصلحة المجتمع الدولي مثل الاستخدام العسكري و الارهابى أو كوسيط في العمليات العدائية أو الصراع المسلح كل ذلك من شانه الإضرار الجسيم بالأمن والسلم الدوليين ويأتي في اطار ذلك ايضا الجهود الدولي في مكافحة ارهاب اختطاف الطائرات وحماية المجال الجوي للملاحة المدنية .

ويعبر كل من الفضاء الخارجي والفضاء الإلكتروني عن منطقة هامة للمجتمع الدولي حيث يحوى الفضاء الخارجي الأقمار الصناعية الخاصة بالاتصالات والأغراض العلمية والطقس ونظم الإنذار وأقماراً أخري للتجسس والأغراض العسكرية، كما يحوي الفضاء الخارجي مجالا للطاقة يمكن أن تستخدم في الأغراض السلمية، ويقدم قانون الفضاء الخارجي أطراً هامة حول تنظيم استخدام الفضاء الخارجي في الأغراض السلمية والعمل على منع استخدامه في الأغراض العسكرية، وأدى ظهور هذا النشاط الجديد للإنسان وتطوره بهذه السرعة إلى ظهور قانون فضاء ذي طبيعة خاصة ومتميزة، يتناول الطبيعة القانونية للفضاء الخارجي و- النظام القانوني الذي يحكم استخدام الفضاء الخارجي. وطبيعة المشكلات التي تنتج عن استخدام الفضاء الخارجي.[1] وتظهر أهمية الاستخدامات السلمية للفضاء الخارجي من حيث إنها ذات طبيعة إستراتيجية وتجارية وعلمية، وهي تدفع المجتمع الدولي للاهتمام بهذا المجال وتطويره بما يعزز التعاون الدولي، كما أن المعركة نحو فضاء مستقر قائم على المساواة بين الدول لا يمكن تحققه إلا إذا تضافرت

---

(1) بن حمودة ليلي ،" الاستخدام السلمي للفضاء الخارجي،"، المؤسسة الجامعية للدراسات والنشر ،الجزائر ، الطبعة الأولى ، ٢٠٠٧،ص ص ٢٣٤- ٥٩٢.

الجهود التكنولوجية لكل الدول وعلى المدى البعيد، بالإضافة إلى ضرورة العمل المشترك والتعاون الدولي من أجل إبعاد الفضاء الخارجي والقمر والأجرام السماوية من التسلح ومن النزاعات المسلحة، وبخلاف الفضاء الخارجي الذي لا يتجاوز عدد الدول التي تمتلك قدرات فضائية ٥٢ دولة فان الفضاء الإلكتروني ترتبط به اغلب الدول في العالم سواء أكانت دولاً نامية أو متقدمة بما يعطي زخما اكبر للاستخدامات المتعددة من جانب العديد من الدول.

أولا: القانون الدولي للفضاء الخارجي والأجرام السماوية:

نشا القانون الدولي للفضاء الخارجي والأجرام السماوية عام ١٩٦٧ وهو المقصود به القانون والتشريع الذي يتحكم في الرحلات الفضائية ومرور المركبات الفضائية فوق أجواء الدول ومياهها الإقليمية، وقد بدأ النظر في القانون الفضائي في الستينات من القرن العشرين الماضي علماً أن القانون الذي يحكم الرحلات الجوية بالطائرات قد سبق ذلك وقررت الدول المشاركة في مؤتمر اعد لذلك وانبثقت فكرة المجال الجوي وهو الفضاء الواقع فوق الدولة والذي تنتهي حدوده مع حدودها الطبيعية أو حدود مياهها الإقليمية، وعقد أول مؤتمر دولي لبحث هذا الأمر، وتقدم بعض المشرعين باقتراح اعتبر في حينه حلاً للمشكلة وذلك بتطبيق مادة من مواد التشريع الروماني التي تنص فيه على أن من يمتلك الأرض يمتلكها عالياً حتى السماء، واسقط هذا الاقتراح بسبب أن القانون الروماني جعل لمن أراد أن يزيد في ادوار بيته باتجاه السماء، وبعد عدة مداولات انتهوا إلى أن ملكية الدولة للفضاء القائم فوقها تنتهي من حيث الارتفاع عند النقطة التي لا تستطيع نيرانها المضادة للطائرات أن تتجاوزه وبنوا ذلك على نص القانون الدولي حول سيادة الدول على أراضيها بـ " إن السيادة الإقليمية للدولة تتوقف عند الحدود التي يستطيع حكامها ممارسة القوانين المعمول بها، وذود جميع الأمم الأخرى عنها".[1]

وتقدم بعض المسئولين الأمريكيين بأن حقوق الفضاء لأي دولة تتوقف عند ارتفاع محدد وحددوا ٤٠ /٥٠ / ٨٥كيلو متراً والبعض حدد نهاية الجاذبية الأرضية والبعض حدد بانعدام الجزيئات الجوية، وفي ٢٢ نوفمبر١٩٦٣م تقدم رئيس لجنة الفضاء المنبثقة عن الأمم المتحدة بمشروع يبين الحقوق الفضائية للدول ووافق عليه ممثلو الأمم المتحدة بما في ذلك ممثلو الاتحاد السوفيتي وأمريكا، وجاء فيه إن الفضاء الخارجي الواقع خارج الجو الأرضي وكذلك الأجرام السماوية لا تخضع لأحكام السيادة القومية.

ويجب كذلك أن يكتشف الفضاء خارج جو الأرض لصالح الإنسانية وان سائر الدول تعتبر الملاحين الكونيين سفراء للبشرية جمعاء.، وقد عانى المشرعون من صعوبات في إعداد قانون الفضاء الخارجي منها: أولاً-الارتفاع الشاهق الذي تصل إليه المركبات الفضائية والمسافات الطويلة التي تقطعها هذه المركبات الفضائية في رحلاتها، ثانياً-الطريقة التي تنطلق بها المركبات الفضائية والتي تجعلها تدور حول الكرة الأرضية كلها عند الصعود للفضاء وعند الهبوط على الأرض وعدم انطلاقها نحو الفضاء مباشرة في طريق مستقيم، ثالثاً-الأقمار الصناعية تحتاج إلى مواقع خاصة ومدارات محددة للقيام بنشاطاتها سواء في الاتصالات أو البث التلفزيوني أو مراقبة الطقس ونحوه، وقد نصت اتفاقية ١٩٦٧ في المادة الثانية على أنه "لا

---

(1) مرجع سابق ذكره .

يجوز التملك القومي للفضاء الخارجي بما في ذلك القمر والأجرام السماوية الأخرى بادعاء السيادة أو عن طريق الاستخدام أو وضع اليد أو الاحتلال أو بأي وسيلة آخرى ".

وقد تميزت اتفاقية ١٩٦٧ بأنه لم يتم الإشارة إلى عامل الأمن في التنظيم القانوني للفضاء الخارجي، وذلك لم يرجع لعدم أهميته وإنما يرجع لارتباطه بالجاسوسية من الفضاء، ومن ثم فان أي نشاط سيتم في الفضاء الخارجي تشعر الدولة الضارة انه يخل بأمنها إلى الدرجة التي تعده نشاطا غير مقبول فالمرجح أنها ستعارضه، وان مبدأ قبول الدول لحرية الفضاء الخارجي وتنازلها عن مبدأ السيادة لم يصاحبه تنازل مماثل عن حقوقها الثابتة فيما يتعلق بالحفاظ على أمنها، ونصت الاتفاقية في مادتها الأولى على "أنه لكافة الدول حرية استكشاف واستخدام الفضاء الخارجي بما في ذلك القمر والأجرام السماوية دون تمييز وعلى قدم المساواة وفقا للقانون الدولي "، و نصت المادة الثالثة على أن الدول الأطراف في المعاهدة ملتزمة في مباشرتها لأنشطتها في ميدان استكشاف واستخدام الفضاء الخارجي بما في ذلك القمر والأجرام السماوية الأخرى بمراعاة القانون الدولي بما في ذلك ميثاق الأمم المتحدة بغية صيانة السلم والأمن الدولي " [1].

وقد مثل إعلان المبادئ القانونية لكشف واستخدام الفضاء الخارجي في ١٣ ديسمبر ١٩٦٣ أول وثيقة تاريخية تتضمن تنظيما قانونيا مكتوبا للمشاكل الناجمة عن أنشطة الدول في الفضاء الخارجي، وحمل هذا الإعلان عدداً من المبادئ الهامة التي يمكن الاستفادة منها في مجال التعامل مع ظاهرة الفضاء الإلكتروني ومن أهم تلك المبادئ إن تكرس أنشطة الدول في كشف واستخدام الفضاء الخارجي لصالح البشرية جمعاء، وان حرية كشف واستخدام الفضاء الإلكتروني والإجرام السماوية على أساس المساواة بين الدول وفقاً للقانون الدولي، وأن هناك عدم قابلية للفضاء الخارجي والإجرام السماوية للتملك من جانب أي دولة، وان الدول في أنشطتها المتعلقة بكشف واستخدام الفضاء الخارجي تلتزم بقواعد القانون الدولي بما في ذلك ميثاق الأمم المتحدة، كما إن الدول التي تطلق أي شيء في الفضاء الخارجي مسئولة دولياً عن الضرر الذي يصيب دولة أجنبية من هذه الأشياء أو من الأجزاء المكونة لها على الأرض أو في الفضاء الجوي أو الخارجي [2].

وترسخ الاتفاقية الدولية للفضاء الخارجي والإجرام السماوية لعام ١٩٦٧ مفهوم التراث المشترك للإنسانية وكيفية التعامل مع الفضاء الذي لا يخضع لملكية احد، وتنص المادة الأولى من الاتفاقية على " أن يكون كشف واستخدام الفضاء الخارجي بما في ذلك القمر والأجرام السماوية لخدمة صالح كافة الأعضاء بغض النظر عن درجة تقدم كل منها اقتصاديا أو علميا والفضاء ميدان للبشرية جمعاء " [3] وفي الفقرة الثانية " من المادة نفسها "مبدأ حرية كشف واستخدام الفضاء الخارجي والأجرام السماوية لكافة الدول على أساس حق المساواة بينها وفقاً للقانون الدولي "، أما المادة الثانية من الاتفاقية فتنص على " عدم خضوع الفضاء الخارجي بما في ذلك القمر والأجرام السماوية للتملك أو السيطرة عن طريق الاستخدام أو الاحتلال أو أي وسيلة أخرى [4] ".

---

(1) علي صادق عبد الحميد صادق، " امن الدولة في النظام القانوني للهواء والفضاء الخارجي "، رسالة دكتوراه، كلية الحقوق جامعه القاهرة، ١٩٧٩، ص ص ٢٥-٨٨ .

(2) منى محمود مصطفى، "الجوانب القانونية والسياسية لمشاكل الفضاء الخارجي "، رسالة دكتوراه، كلية الاقتصاد والعلوم السياسية، جامعه القاهرة، ١٩٧٥ ص ص ١٤٦-٢١٨ .

(3) الاتفاقية الدولية للفضاء الخارجي والأجرام السماوية عام ١٩٦٧، المادة الأولى والثانية.

(4) منى محمود مصطفى، "الجوانب القانونية والسياسية لمشاكل الفضاء الخارجي "، مرجع سابق ذكره ص ص ٣٠٦ - ٣٦٠

ثانيا: الفضاء الخارجي والاستخدام غير السلمي

أصبحت استخدامات الفضاء محل اهتمام كافة الدول سواء في الاستخدامات السلمية أو في العمل العسكري، حيث أصبح الفضاء الخارجي جزءاً هاماً من العمل العسكري واحتمال أن يلعب دورا هاما في الصراعات ذات الطابع العسكري العنيف أو ذات الطابع الممتد مع دخول الفضاء الخارجي ساحة الاتصالات والتكنولوجيا والأقمار الصناعية وتأثير ذلك على الأمن والاقتصاد الدولي، و أصبحت القوة في الفضاء الخارجي مجالا للتنافس بين القوى الكبرى لتحقيق عناصر القوة به وارتكزت عناصر القوة على نظرية "ويرج" عن القوة الفضائية James Oberg في كتابة "نظرية قوة الفضاء " إلى وضع نظام متماسك يعظم القوة الفضائية والتي حددها اويرج على أنها تعني " مجموع التقنية والسكان والاقتصاد والصناعة والقوة العسكرية وإرادة الدولة وغيرها من العوامل التي تساهم في دعم إمكانيات الدولة على ممارسة الإكراه أو الإقناع أو ممارسة التأثير السياسي على الدول الأخرى بغرض الوصول إلى الأهداف الوطنية من خلال القدرات الفضائية "(1).

و أصبح الفضاء الخارجي مسرحاً لممارسة القوة التي تبقى عاملا رئيسيا في اتخاذ القرار المتعلق بالصراع العسكري وسيكون العنصر الحاسم في المستقبل، كما إن أي دولة ذات قوة فضائية يمكن أن تكون عرضة لتعرض إمكانياتها للهجوم أو تصبح هدفاً في حالة النزاع المسلح، وسيكون لمسالة الهجوم تأثيرات ليس فقط على القدرات الفضائية بل كافة الأنظمة المرتبطة بها من الاستخدامات السلمية ذات الطابع المدني، وأن العوامل السياسية والاقتصادية سيكون لها تأثيراتها على المجتمع الدولي، وأي هجوم سيكون له تأثيرات تمس الأمن الجماعي وان مسالة منعه من الحدوث أو مناهضة عسكرة الفضاء كإجراء وقائي للأمن الدولي. (2)

ويأتي هذا مع تعاظم الاعتماد على الفضاء الخارجي في الاستخدامات السلمية من خلال تداخله مع نظم الاتصال والإعلام فضلا عن تنامي دوره في المستقبل في تقديم خدمات الإنترنت وما يمثل ذلك من مصلحة إستراتيجية دولية، مع زيادة عدد الدول المالكة للأقمار الصناعية وإشكالية علاقة هذه الدول ما بين العداء أو التحالف و مسالة تفعيل الاستخدام الفعلي لتلك الأقمار، وصعوبة الفصل بين الطابع السلمي والعسكري. وتطرح مسالة إطلاق الدول الكبرى للأقمار الصناعية سواء للإغراض السلمية أو العسكرية إشكالية الاستخدام العسكري للفضاء واثر ذلك على المنشئات المدنية والحيوية في العالم. ولعل تلك المسالة كانت قد أثيرت إبان الحرب الباردة فيما يسمي "بحرب النجوم " إلا أن تربع الولايات المتحدة على عرش القوة الدولي قد دفع بدول أخرى لخوض مجالات الفضاء وهذا ما قد يشكل تحديا مستقبليا بين تلك القوة، وخاصة مع تأكيد الولايات المتحدة أنها سترد بقوة ضد إي محاولات لإعاقة أنشطتها في الفضاء الخارجي (3) وتتخذ خطوات وتدابير وقائية ضد أي محاولة ضدها في الفضاء سواء أكانت من قبل دول منافسة أو جماعات

---

(1) Brent D. Ziarnick ," The Space Campaign: Space-Power Theory Applied to Counterspace Operations, Air & Space Power Journal - Summer 2004 (http://www.airpower.maxwell.af.mil/airchronicles/apj/apj04/sum04/ziarnick.html#ziarnick)

(2) على صادق عبد الحميد صادق، " امن الدولة في النظام القانوني للهواء و الفضاء الخارجي "، مرجع سابق ذكرة ،ص ص ٨٥-١٢٣.

(3) جريدة الأهرام ١٨- ١٢- ٢٠٠٦.

إرهابية، ويأتي هذا مع رفض الولايات المتحدة بدء مباحثات حول التسلح في الفضاء تحت رعاية الأمم المتحدة، وتزداد خطورة التصعيد العسكري في الفضاء مع صعود الصين كقوة في الفضاء الخارجي بل وعزمها إقامة قاعدة لها دائمة على سطح القمر إلى جانب روسيا والقوى الأخرى، وتطرح قضية السيطرة على الفضاء الخارجي إمكانية السيطرة على مجال الاتصالات الدولية والتي تتجه إلى الاعتماد المتزايد على الأقمار الصناعية وليس فقط المحطات الأرضية، وتزايد الأهمية الإستراتيجية للفضاء الخارجي لكافة القوى الدولية وظهور مشكلة مخلفات المحطات الفضائية.

ثالثا: تزايد حجم الاعتماد الوظيفي ما بين الفضاء الخارجي والالكتروني.

تحمل مسألة التداخل بين الفضاء الخارجي والفضاء الإلكتروني تحديات تتعلق بإمكانية تعرض الفضاء الخارجي وما يحمله من أقمار صناعية إلى الخطر من جراء تعرضه إلى:الهجوم المادي: وهو الهجوم الذي يترك أثرة التدميري الفعلي بهدف تعجيز أو تحطيم العدو لتحقيق خسائر مادية وكذلك في الأرواح حيث تصبح الأقمار الصناعية وسيلة من وسائل الحرب التقليدية. وهناك الهجوم على المعلومات: حيث يتم مهاجمة وسائل وأجهزة الاتصالات بهدف تحقيق نتائج الهجوم المادي ويأخذ هذا النوع من الهجوم أشكالا عديدة مثل عمليات التشويش على أجهزة اتصالات الأقمار الصناعية ومحطاتها الأرضية كذلك إرسال إشارات مشوشة إلى الأقمار الصناعية المعادية وتلويث أجهزة الكمبيوتر والمحطات الأرضية بالفيروسات لشل قدراتها على إرسال المعلومات.

وهناك الهجوم على المرافق العامة والمنشآت: حيث يشمل التعرض للأقمار الصناعية أو التعرض لمرافق الفضاء وقواعده الأرضية وهذه المنشآت هي هدف للسيطرة الفضائية لأنها نادرة الشكل وثابتة المكان ويمكن مهاجمتها بالطرق التقليدية. وهناك الهجوم على المراكز الصناعية: حيث يتم استنزاف الدعم الصناعي لقوة الدولة الفضائية بما يؤثر على جهودها وتعطيل العمل في تطويرها أو دعمها بالإضافة إلى الهجوم على المعدات الثقيلة الخاصة بالأجهزة الفضائية: حيث يستهدف الهجوم مهاجمة المعدات والأدوات ذات الاستعمال الفضائي الثابتة على الأرض وذلك بهدف إزالة القدرات الفضائية للدولة الخصم وذلك بسبب صعوبة صنع أو إصلاح جزء، وكذلك فان هذا الهجوم يمكن إن يتم عن طريق استخدام الأسلحة ذات الحركة النشطة حيث تكون أكثر فاعلية ضد أجهزة الكمبيوتر بما يتسبب في الاختناق الالكتروني للأجهزة دون أضرار مادية، و اعتبر الفضاء الإلكتروني مجالا جديدا في العلاقات الدولية.[1]، وذلك بعد انتقال مجالات الحياة المختلفة إلية إلى الدرجة التي شبه البعض بالفضاء الخارجي إلى الدرجة التي جعلت من

---

[1] في ٢٨ يونيو ٢٠٠٧ أسست وكالة ناسا جزيرتين جديدتين في الموقع الإلكتروني الشهير المسمى (سلكند لايف) أي العالم الثاني. ويستطيع أي شخص مهتم بالترحال في الفضاء أو عالم التكنولوجيا، أن يزور الجزيرتين بغرض الاستكشاف والمساهمة في المهمة التي تؤديها وكالة أبحاث الفضاء الأميركية (ناسا).و أطلق على إحدى الجزيرتين اسم (كولاب) وهو اسم مختصر للمختبر التعاوني لاستكشاف الفضاء، وقد أنشأ أو أسس الجزيرة في العام ٢٠٠٦ مركز (إيمز) للأبحاث التابع لناسا الموجود في المنطقة المعروفة باسم وادي السليكون بولاية كاليفورنيا. وقد تأسست الجزيرة لتكون مجتمعا افتراضيا تعليميا يحتوي على مواد تتيح لزوار الموقع التفاعل معه. وبالقرب من الجزيرة الافتراضية الأولى تقع الجزيرة الافتراضية الثانية واسمها (إكسبلورار) وهذه الجزيرة تأسست خلال علم ٢٠٠٨ بمختبر الدفع النفاث التابع لناسا أيضا في معهد التكنولوجيا بولاية كاليفورنيا. ويعتبر مختبر الدفع النفاث المركز الرائد بالولايات المتحدة لاستكشاف النظام الشمسي بأجهزة الروبوت.

بعض العلماء يستخدمون تعبير الثقوب السوداء في الفضاء الإلكتروني على نسق الفضاء الخارجي وإنها تقوم بدورها حين تبتلع الرسائل والبيانات الالكترونية. [1]

رابعا: سباق التسلح في الفضاء الخارجي والالكتروني:

يعد من تحديات الفضاء مخاطر تهديدات الأسلحة الفضائية، وكذلك الشظايا المتخلفة عن بقايا الأقمار الصناعية والسفن الفضائية، وما يتعلق بتأثيرها على أمن البشرية، مع احتمال تزايد أخطار الشظايا والأسلحة الفضائية على عمل النظم التكنولوجية الخاصة بالأرصاد الجوية وشبكات الاتصالات [2]، والاختبارات العسكرية كالتي أجرتها الصين في بداية عام ٢٠٠٧ م لاختبار ضربات مضادة للأقمار الصناعية، وما زالت تعارض الولايات المتحدة في فرض قيود للحد من تطوير أسلحة فضائية، وانعكاس ذلك على تفكيك الفضاء بوصفه حرما للأقمار الصناعية في ميدان الاتصالات والأرصاد الجوية، وللأجهزة الأخرى التي يعتمد عليها اقتصاد العالم بشكل كبير، وبالتالي تحويله إلى موقع يستحيل على هذه الأجهزة العمل فيه.

وبما سيؤثر سلبا على كل فرد من سكان العالم، حيث سيتم شل عمل أجهزة تكنولوجيا الاتصال والمعلومات كالإنترنت والهاتف أو أجهزة التراسل وموجات الراديو والتلفزيون و أصبحت العلاقة بين الفضاء الخارجي والفضاء الالكتروني وثيقة الصلة وتزداد تطورا وأهمية في المستقبل حيث بروز أنظمة الأقمار الصناعية في الأغراض الاتصالية والعسكرية والعلمية، حيث يتزايد الاعتماد عالميا على الأقمار الصناعية في الاتصالات بالإضافة إلى دخول دول عديدة المعترك لتتنافس عمليا وعسكريا في الفضاء في ظل هيمنة أمريكية على كل من الفضاء الالكتروني والفضاء الخارجي وتحاول عدة دول صاعدة على المسرح الدولي اختراقها [3].

وبرزت محاولات دبلوماسية أحيانا وأخرى عسكرية أحيانا أخرى، لدفع الولايات المتحدة للتنازل عن سيطرتها على شبكة الإنترنت وإعطاء دور للأمم المتحدة في إدارتها، أما على صعيد الفضاء الخارجي فانه على الرغم من تقدم الجهود الدولية في سبيل تنظيم استغلال الفضاء الخارجي والأجرام السماوية والتي تمثلت في قانون الفضاء الخارجي والأجرام السماوية لعام ١٩٦٧، فان تطبيقها شكل تحديا من جانب القوى الكبرى المهيمنة على النظام الدولي سواء أكان في فترة الحرب الباردة فيما عرف بحرب النجوم، أو بعد انهيارها وظهور الولايات المتحدة كقطب أوحد ليلقى هو الأخر تحديا من جانب بعض القوى الدولية من اجل الدفع نحو تعدد قطبيه النظام الدولي وأظهرت الهيمنة الأمريكية على الفضاء وضعا شبيها بالهيمنة البريطانية علي البحار في القرن التاسع عشر والتي أفرزت الاتفاقية الدولية لقانون البحار عام ١٩٨٢.

وعلى الرغم من أن كلا من الفضاء الالكتروني والفضاء الخارجي هي ملك وتراث مشترك للإنسانية، إلا إن هناك محاولات لإخضاع ذلك لاعتبارات القوة والاعتبارات السياسية، وظهر التداخل والاعتماد المتبادل

---

(1) Clara Moskowitz ," **Internet Full of 'Black Holes'**", .livescience.com, 2008-04-11. (http://www.livescience.com/technology/080411-cyber-black-holes.html.)

(2) جريدة الشرق الأوسط ١٦ سبتمبر ٢٠٠٧.

(3) د.محمد بهي الدين عرجون، " الفضاء الخارجي واستخداماته السلمية "، سلسلة عالم المعرفة، عدد ٢١٤، المجلس الوطني للثقافة والفنون والاداب، الكويت، أكتوبر ١٩٩٦،ص ص ١٧٧-٢٦٧ .

بين شبكة الإنترنت والفضاء الخارجي من خلال بروتوكولات الاتصالات عن طريق عدد من الشبكات التي تحتوي خاصية تبادل الملفات وهي شبكة راديو متنقلة ونظام تبادل بيانات عن طريق الاتصال بالأقمار الصناعية مع إمكانية استخدام أنواع البروتوكولات الخاصة بالإنترنت لدعم الاتصالات مع مركبات الفضاء التي تتحرك حول النظام الشمسي، وأصبح الإنترنت لا يعتمد فقط على الشبكات الأرضية مع وجود مبادرات لاعتماد الاتصال بالإنترنت عبر الأقمار الصناعية، وقد انتهجت وزارة الدفاع الأمريكية على تدشين مشروع توجيه الإنترنت عبر الفضاء عن طريق الأقمار الصناعية، في بداية عام ٢٠٠٩.[1]

ويوجد نوعان لإرسال المعلومات من جهاز المستخدم إلى الأقمار الصناعية، إمّا باستخدام وسيلة اتصال أخرى للإنترنت لطلب الصفحات مثل "دي إس إل" Upload أو استخدام جهاز مباشر لإرسال المعلومات إلى الأقمار الصناعية Multiway. وهناك مشروع اوروبي اسمه "يونيك" Universal satellite home Connection UNIC يهدف لتقديم خدمات الإنترنت عالي السرعة والتلفزيون للمنازل عبر الأقمار الصناعية، واستقبال وإرسال المعلومات من وإلى الأقمار الصناعية. وبدأ هذا المشروع في فبراير ٢٠٠٦، وانتهى في يوليو ٢٠٠٨. ومن الشركات التي تقدّم خدمات الإنترنت عبر الأقمار الصناعية للمنطقة العربيّة "أوربت" Orbit و"عربسات"[2] ويسعى البنتاجون لتنفيذ مشروع عالي التقنية أطلق علية اختصاراً "ايرس" Internet Router In Space-Iris للاتصالات العسكرية والتي ربثما ما قد تتحول إلى الاستخدامات المدنية، كما كان الحال بالنسبة إلى شبكة اربانت العسكرية والتي أصبحت نواه لابتكار الإنترنت، والذي استخدمه وزارة الدفاع الأمريكية للاتصالات العسكرية في ستينات القرن العشرين.

والتي تحولت بمرور الوقت من مراحل التطور لتصل إلى الامتداد والتوسع في البرامج والمعدات وانفتحت على المجالات المدنية ولم تعد مقصورة على العسكرية فقط، كما أصبحت متاحة للجميع ، ومن شأن ذلك تحول الفضاء الالكتروني لكيان فضائي ، وتطويرا للجهود التي تتم في مجال الإنترنت عبر الأقمار الصناعية وكان لابد من مرورها وتوجيهها عبر موجات أرضية في محطات أرضية ومن ثم يتحتم للاتصالات الانطلاق من الأرض إلى القمر الصناعي ثم العودة للتوجيه ثم إلى القمر الصناعي ثم إلى الأرض أخيرا، ولكن باستخدام نظام ايريس سوف يتم اختصار الوقت وضمان كفاءة الاتصال بعدم مرورها إلى الأرض للتوجيه وإجرائه مباشرة بين الأقمار الصناعية، ولتشكيل منظومة متقدمة تمكن الأقمار الصناعية والطائرات وسفن الفضاء والمعدات المتقدمة والأنظمة العسكرية الأخرى من التنسيق والاتصال بفاعلية.[3]

---

(1) John Blau, **"US military plans to put Internet router in space"**, IDG News Services, April 12, 2007

(2) جريدة الشرق الأوسط، ١٢-٢-٢٠٠٨.

(3) المبدأ ١، ٧، من إعلان المبادئ .

## المطلب الثاني:

## الفضاء الإلكتروني واتفاقية القانون الدولي للبحار لعام ١٩٨٢

هناك علاقة تحمل بعدين هامين بين البحار والفضاء الإلكتروني الأول يتعلق بان تلك البحار تحمل في قيعانها ما يزيد على ٩٥ ٪ من الكابلات البحرية التي يتم من خلالها الاتصال وتوفير خدمات الإنترنت، من خلال الألياف البصرية التي ما زالت تتميز عن الاتصال بالأقمار الصناعية بسرعتها، إما البعد الثاني فيتعلق بالجهود الدولية الخاصة بالمعاملة القانونية مع أعالي البحار ومنطقة التراث المشترك للإنسانية والجهود الدولية لمكافحة القرصنة البحرية التي عملت على ترسيخ فكرة الأمن الجماعي والمرفق الدولي الذي يهتم بها كل أطراف المجتمع الدولي من اجل الحفاظ على امن أعالي البحار وحماية الاستخدام السلمي لها.

أولا :منطقة التراث المشترك للإنسانية:

تم إرساء هذا المبدأ منذ قرار الجمعية العامة للأمم المتحدة في ١٧ ديسمبر ١٩٧٠ والمعنون بـ " إعلان المبادئ المنظمة لقاع البحار والمحيطات وباطن أرضها خارج حدود الولاية الوطنية " وأقرت الجمعية العامة للأمم المتحدة إن منطقة قاع البحار والمحيطات وباطن أرضها التي تقع خارج إطار الولاية الوطنية للدول هي ومواردها تعد تراثا مشتركا للإنسانية وان استكشافها واستغلالها يجب إن يكون لصالح الإنسانية جمعاء بصرف النظر عن الموقع الجغرافي للدول[1]. وجاء هذا الإعلان ليتم التأكيد علية وتطويره في الاتفاقية الدولية للبحار ١٩٨٢ وملاحقها ١٩٩٤.

وجاء ذلك بعدة مبادئ خاصة بتلك المنطقة التي تعد ضمن التراث المشترك للإنسانية، وانه ليس لأية دولة أن تدعي ملكيتها أو تمارس حقوقها السيادية على أي جزء من المنطقة أو مواردها، وليس لأية دولة أو شخص طبيعي أو اعتباري الاستيلاء على إي جزء من المنطقة، كما أن الأنشطة التي يتم إقامتها في تلك المنطقة تكون لصالح الإنسانية جمعاء بصرف النظر عن الموقع الجغرافي للدول وتكون المنطقة مفتوحة لاستخدامها للإغراض السلمية دون غيرها، وان يتم اتخاذ التدابير اللازمة لضمان الحماية الفاعلة للبيئة البحرية من الآثار الضارة التي قد تنشا من بعض الأنشطة غير القانونية في المنطقة وان يتم حفظ الأشياء ذات الطابع الأثري أو التاريخي التي يعثر عليها في المنطقة أو يجرب التصرف فيها لصالح الإنسانية جمعاء[2].

وعمل القانون الدولي على تحديد حدود منطقة التراث المشترك للإنسانية والنظام القانوني الخاص بها والمنظمة الدولية التي تعنى بإدارة هذه المنطقة فيما أطلق علية بـ" السلطة الدولية "، والتي تعد منظمة دولية تمارس من خلالها الدول الأطراف الأنشطة التي يتم ممارستها في المنطقة وكذلك الرقابة عليها ويوجد مقر تلك السلطة في جامايكا وقد بدا العمل بها في ١٦ نوفمبر ١٩٩٤ وتم تحديد الشخصية القانونية لها والاختصاصات والنظام المالي والحصانات والامتيازات وطبيعة هيكلها الاداری، وهي سلطة تنظم تلك الأنشطة، وعليها أن تحقق التقاسم العادل للمنافع المالية والمنافع الاقتصادية الأخرى

---

(1) U.S. Military to Put Internet Router in Space, SPACE.com staff ", 13 April 2007

(2) وائل احمد علام، " الاتفاق التنفيذي لاتفاقية قانون البحار "، دار النهضة العربية، القاهرة، ٢٠٠١، ص ص ٨-١٠ .

المستدامة منها وتفرض الاتفاقية على السلطة الدولية لقاع البحار واجب اتخاذها للتدابير اللازمة فيما يتعلق بالأنشطة فـــي " المنطقة "، التي ترمي إلى منع التلوث وخفضه والتحكم به، والأخطار الأخرى المحدقة بالبيئة البحرية، وحماية الموارد الطبيعية لها وصونها.

ثانيا: منطقة أعالي البحار:

هناك أيضا إسهام آخر للقانون الدولي للبحار يتعلق بترسيخه لمنطقة أعالي البحار وهي تلك المنطقة التي لا تكون جزءا من الامتداد البحري الخاضع لسيادة الدولة الساحلية، وبتواجد البحر العالي فيما وراء المساحات البحرية كالمياه الداخلية والبحر الإقليمي والمنطقة المتاخمة والمنطقة الاقتصادية الخالصة، وتكون القاعدة العامة في أعالي البحار أنها مفتوحة لكل الدول ساحلية أو غير ساحلية وتتميز بعدم أحقية أية دولة في أن تدعي سيادتها على أعالي البحار.

كما لا يجوز للدول أن تقيم عليها أي قواعد عسكرية حيث تم فقط استخدامها في الأغراض السلمية. وان لكل الدول حق في تسيير السفن الخاصة بها برفع علمها عليها، وهناك حريات تتعلق بحرية الصيد وحرية التحليق الجوي وحرية البحث العلمي والصيد وحرية وضع الكابلات البحرية وخطوط الانانيب تحت الماء على قاع البحار كما ورد في المواد (١١٢، ١١٣، ١١٤، ١١٥) والتأكيد على ضرورة خضوع كل دولة للقوانين واللوائح التي تكفل معاقبة كل قطع أو تدهور للكابلات، وللدول الحق في التعويض عن الضرر[1].

ولاقي مبدأ التراث المشترك للإنسانية قبولاً عاماً لدى المجتمع الدولي، وأصبح له دور في التنمية العالمية ودعم الأمن الإنساني بإبعاده الاقتصادية والسياسية والأمنية، وتم إقرار هذا المبدأ في طريقة التعامل الدولي مع أعماق وأعالي البحار والفضاء الخارجي والقطب الجنوبي وتلك المناطق الخارجة عن حدود السيادة الإقليمية[2].

وقد انشأ المجتمع الدولي ما عرف بمرفق السلطة الدولية لقاع البحار حيث انه وفقا للاتفاقية الأمم المتحدة لقانون البحار التي تم إبرامها في عام١٩٨٢ يمثل قاع البحار والمحيطات وأرضها خارج نطاق الولاية الوطنية هي ومواردها تراثا مشتركا للإنسانية ويتم استكشافها واستغلالها لمصلحة الإنسانية جمعاء التي تتصرف السلطة الدولية لقاع البحار لصالحها، وأرسى القانون الدولي للبحار في نسخته المعدلة لعام ١٩٨٢ عدداً من المبادئ التي يمكن النظر من خلالها إلى كيفية وضع قواعد وضوابط لاستخدام الفضاء الإلكتروني وأول هذه المبادئ عدم السيادة على المياه الدولية، والثاني مبدأ شيوع الثروة، والثالث الاستغلال السلمي للثروات، والرابع مبدأ عدم التعدي على حدود الدولة الساحلية، والخامس مراعاة المصالح والحاجات.، والسادس مدى تغير قواعد استغلال المياه الدولية من السلم إلى الحرب واستخدمت اتفاقية الأمم المتحدة لقانون البحار نظاما جديدا لاستغلال الثروات الكامنة في

(1) احمد أبو الوفا ،"القانون الدولي للبحار على ضوء أحكام المحاكم الدولية والوطنية وسلوك الدول واتفاقية ١٩٨٢ "، دار النهضة العربية ، القاهرة ، ٢٠٠٦ ، ص ص ٣٣٠-٣٩٠ .

(2) د. سامي احمد عابدين، "مبدأ التراث المشترك للإنسانية:دراسة قانونية لأعماق البحار والفضاء الخارجي والقطب الجنوبي "، دار النهضة العربية، ١٩٨٦ ص ٤٧٧ .

قيعان المحيطات والبحار، فيما وراء حدود ولاية واختصاص الدولة الساحلية في أعالي البحار المتواجدة بعد المنطقة الاقتصادية الخالصة والجرف القاري للدولة الساحلية،

وفي المادة ١—١ تعرف المنطقة بأنها " قاع البحار والمحيطات وباطن أرضها خارج حدود الولاية الوطنية " وهي تقع في البحار العالية وهي تلك الأجزاء من البحار التي لا تقع داخل المياه الإقليمية أو المنطقة الاقتصادية الخالية أو الجرف القاري.[1]

وقد تميزت ملامح تلك المنطقة القانونية باقتصار استغلال مواردها المعدنية، واستخدام تلك المنطقة في الإغراض السلمية والبحث العلمي والبحري وحماية الحياة البحرية ، و قدمت الاتفاقية الدولية بشأن القارة القطبية لعام ١٩٥٩ كيفية تنظيم الاستخدام السلمي لها كمنطقة تراث مشترك للإنسانية ومثلت خطوة بناءة في سبيل منع الأنشطة العسكرية وأكدت الاتفاقية على إن القارة القطبية هي منطقة علمية وبحث علمي ويتم استغلالها لصالح البشرية[2].

ثالثا : الجهود الدولية لمكافحة القرصنة البحرية .

لاشك ان الفضاء الالكتروني يواجهه عمليات قرصنة ومتنوعه تأتي على نمط القرصنة البحرية والتي عمل القانون الدولي على تجرم أعمال القرصنة البحرية وتكييفها قانونا بأنها جريمة دولية يعتبر مرتكبها مجرما ضد الإنسانية ، وتعرف اتفاقية الأمم المتحدة لقانون البحار لسنة١٩٨٢ القرصنة في المادة(١٠١) بأنها أي عمل غير قانوني من أعمال العنف أو الاحتجاز أو أي عمل سلب يرتكب لأغراض خاصة من قبل طاقم أو ركاب سفينة خاصة أو طائرة خاصة، ويكون موجها في أعالي البحار، ضد سفينة أو طائرة أخري، أو ضد أشخاص أو ممتلكات علي ظهر تلك السفينة أو علي متن تلك الطائرة، أو ضد سفينة أو طائرة أو أشخاص أو ممتلكات في مكان يقع خارج ولاية أية دولة.[3] وتضمنت المادة(١٠٥) من الاتفاقية النص الخاص بمبدأ الاختصاص العالمي لمحاكمة مرتكبي جرائم القرصنة البحرية،

ومن جهة أخرى هناك قواعد القانون الدولي العام التي تضمنتها معاهدة١٩٨٨ الخاصة بالأعمال غير المشروعة التي يتم اقترافها في البحار، وهذا إلى جانب قواعد القانون الدولي العام التي تضمنتها المعاهدات الدولية المتعلقة بسلامة النقل البحري.و قواعد القانون الدولي العام التي تضمنتها المعاهدات والاتفاقيات الدولية والثنائية المبرمة بين الدول بشأن تجريم أعمال الإرهاب الدولية.. ومحاكمة مرتكبيها ومعاقبتهم، وذلك باعتبار أن جريمة القرصنة البحرية عمل من أعمال الإرهاب. وتأتي التشريعات والقوانين البحرية الإقليمية والوطنية وقوانين العقوبات التي تصدرها الدول.. و ميثاق المحكمة الجنائية الدولية في روما الذي تضمن توصيف الأعمال غير المشروعة.. التي تتطبق في أحد أنواعها علي جريمة القرصنة البحرية.

---

(1) احمد أبو الوفا ،"القانون الدولي للبحار " ، مرجع سابق ذكره

(2) Preamble of the Antarctic Treaty, text available at the National Science Foundation website: http://www.nsf.gov/od/opp/antarct/anttrty.jsp. Last Visited: 10/06/07

(3) د. محيي الدين علي عشماوي ، القانون الدولي وجريمة القرصنة البحرية"، ٢٣-٢-٢٠٠٩ (http://www.al-yemen.org/vb/archive/index.php/t-317920.html )

## المبحث الرابع:

## الفضاء الالكتروني

## وفق القانوني الدولي لحقوق الإنسان

**يتناول هذا المبحث تأثير مواجهه الإرهاب الالكتروني او مكافحته او ممارسته على حقوق الإنسان التي كفلتها الأعراف والمواثيق الدولية وشكل مهددا لنمط جديد من الحقوق يرتبط بالفضاء الالكتروني فيما يعرف بحقوق الإنسان الرقمية ، وأصبح المجتمع الدولي يقع في إشكالية مطالب الأمن والحرية ، واستعرض الباحث ذلك عبر المطلب الأول: الإرهاب الالكتروني وحقوق الإنسان الرقمية ، وتناول المطلب الثاني: مكافحة الإرهاب الالكتروني بين مطالب الأمن والحرية**

### المطلب الأول:

### الإرهاب الالكتروني وحقوق الإنسان الرقمية

أصبح التقدم العلمي والتكنولوجي أحد أهم العوامل في تطور المجتمع الإنساني، وعلى الرغم من إتاحته باستمرار فرصا متزايدة لتحسين أحوال معيشة الشعوب والأمم، إلا أنها ولدت في نفس الوقت حالات الاستخدام غير السلمي للفضاء الالكتروني وبما فرض العديد من التحديات الاقتصادية والاجتماعية والسياسية بما يمثل تهديداً كذلك لحقوق الإنسان والحريات الأساسية. وصدرت من الأمم المتحدة والمنظمات الدولية العديدة من الاتفاقيات التي تعمل على تعزيز حقوق الإنسان والأمن الدولي.[1]

وجاءت العديد من الأطر القانونية التي تدعم حقوق الإنسان كالإعلان العالمي لحقوق الإنسان لعام ١٩٤٨، والعهد الدولي الخاص بالحقوق المدنية و السياسية، و العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية الذي أقرته الجمعية العامة في ١٦ ديسمبر ١٩٦٦. وجاء الإعلام الخاص بإعلان المبادئ الأساسية بشان إسهام وسائل الإعلام في دعم السلام والتفاهم الدولي، وتعزيز حقوق الإنسان، ومكافحة العنصرية والفصل العنصري والتحريض علي الحرب الذي أصدره المؤتمر العام لمنظمة الأمم المتحدة للتربية والعلوم والثقافة "اليونسكو" في دورته العشرين، يوم ٢٨ نوفمبر ١٩٧٨[2].

والذي أقر عدة مبادئ أهمها أن يتم تداول المعلومات بحرية ونشرها علي نحو أوسع وأكثر توازنا وان حرية الرأي والتعبير وحرية الإعلام جزء من حقوق الإنسان وحرياته السياسية بما يمثل عاملاً جوهرياً في دعم السلام والتفاهم الدولي، كما جاء الإعلان الخاص باستخدام التقدم العلمي والتكنولوجي لصالح السلم وخير البشرية، والذي تم تبنيه بموجب قرار الجمعية العامة للأمم المتحدة في ١٠ نوفمبر ١٩٧٥ والذي أكد على إن جميع الدول يجب إن تنهض بالتعاون الدولي لضمان استخدام نتائج التطورات العلمية والتكنولوجية لصالح تدعيم السلم والأمن الدوليين، والحرية والاستقلال، وكذلك لغرض الإنماء الاقتصادي والاجتماعي للشعوب وإعمال حقوق الإنسان وحرياته وفقا لميثاق الأمم المتحدة، والعمل على اتخاذ التدابير الملاءمة لمنع استخدام التطورات العلمية والتكنولوجية، ولاسيما من جانب الهيئات التابعة للدولة، للحد من تمتع الفرد بما له من حقوق الإنسان والحريات الأساسية، كما هي

---

(1) للمزيد يمكن الاطلاع على الاتفاقيات الدولية الخاصة على موقع الأمم المتحدة على الإنترنت على الرابط التالي ( http://www.un.org/Depts/dhl/dhlara/resguida/resins.htm)

(2) حقوق الإنسان: مجموعة صكوك دولية، المجلد الأول، الأمم المتحدة، نيويورك، ١٩٩٣، ص ١٧٤.

مكرسة في الإعلان العالمي لحقوق الإنسان والعهدين الدوليين الخاصين بحقوق الإنسان والصكوك الدولية الأخرى ذات الصلة بالموضوع، أو لعرقلة هذا التمتع. و قضى الإعلان بان علي جميع الدول أن تتخذ تدابير لكفالة جعل المنجزات العلمية والتكنولوجية تلبي الحاجات المادية والروحية لجميع قطاعات السكان. وان تمتنع الدول عن أية أعمال تستخدم فيها المنجزات العلمية والتكنولوجية لأغراض انتهاك سيادة الدول الأخرى وسلامتها الإقليمية، أو التدخل في شؤونها الداخلية، أو شن الحروب العدوانية، أو قمع حركات التحرير الوطني أو تنفيذ سياسة قائمة علي التمييز العنصري. ولا تمثل هذه الأعمال خرقا صارخا لميثاق الأمم المتحدة ومبادئ القانون الدولي فحسب، بل تشكل أيضا تشويها غير مقبول للمقاصد التي ينبغي أن توجه التطورات العلمية والتكنولوجية لخير البشرية، والعمل على اتخاذ التدابير الاجتماعية والاقتصادية وتمكين جميع طبقات السكان من الإفادة من حسنات العلم والتكنولوجيا وإلي حماية هذه الطبقات، اجتماعيا وماديا، من الآثار الضارة التي يمكن أن تترتب علي سوء استخدام التطورات العلمية والتكنولوجية، بما في ذلك إساءة استعمالها علي نحو يمس بحقوق الفرد أو الجماعة، ولاسيما فيما يتعلق باحترام الحياة الخاصة وحماية شخصية الإنسان وسلامته البدنية والذهنية. من خلال تدابير فعالة، بما في ذلك التدابير التشريعية لمنع وتلافي استخدام المنجزات العلمية والتكنولوجية للإضرار بحقوق الإنسان والحريات الأساسية وبكرامة الشخص البشري.[1]، و تم إقرار ذلك في القمة العالمية لمجتمع المعلومات في دورتها الأولى ٢٠٠٣ والثانية في عام ٢٠٠٥، ومن ثم فان استخدام الفضاء الإلكتروني في الأعمال العدائية أو التخريبية يمثل بلا شك انتهاكا للمواثيق الدولية والعرف الدولي وذلك يرجع إلى أهمية الفضاء الإلكتروني كوسيط في تقديم الخدمات للمواطنين .

و أدى بروز الفضاء الإلكتروني إلى وجود نوع ونمط جديد من حقوق الإنسان يرتبط بحرية استخدام أداوت تكنولوجيا الاتصال والمعلومات وكذلك حرية التعبير عن الرأي، وقد أدى دور الفضاء الإلكتروني المتزايد على الساحة و الدولية وتعلقه بتقديم خدمات الصحة والتعليم والخدمات المالية والمصرفية والاتصال إلى ارتباط الحصول علية بحق من حقوق الإنسان الذي تمت الإشارة إليه في مواثيق حقوق الإنسان الدولية، وهذا ما استتبع بظهور حقوق الإنسان الرقمية أو الالكترونية Digital human Rights. ، وظهرت العديد من الاجتهادات التي تحاول تأصيل وتحديد هذه الحقوق، وتمضى هذه الاجتهادات في مسارين، الأول يركز على القضايا والموضوعات ذات العلاقة بالإنترنت وتداول المعلومات داخلها وأحيانا خارجها، والمسار الثاني يركز على القضايا والموضوعات ذات العلاقة بقدرة الإنسان على الاتصال والتواصل مع البيئة المحيطة به عموما من خلال خطوط وشبكات الاتصالات، كالحق في الدخول إلى وسائل الاتصالات وفي الاتصال الشخصي الذاتي والحق في الوصول إلى المعلومات والدخول عليها، والحق في المشاركة الاتصالية، هذا بالإضافة إلى الحق في الخصوصية وحقوق الملكية الفكرية. وحق التعبير عن الرأي والنشر، وتقضي المادة ١٩ من الإعلان العالمي لحقوق الانسان بان "لكل انسان الحق في اعتناق اراء دون مضايقة " وان " لكل انسان حق في حرية التعبير و يشمل هذا

---

(1) حقوق الإنسان: مجموعة صكوك دولية مرجع سابق ذكره، ص ٧٥١

الحق حريته في التماس مختلف ضروب المعلومات و الافكار وتلقيها ونقلها الى الاخرين دونما اعتبار للحدود سواءً على مكتوب او مطبوع او بأية وسيلة يختارها". وطرح ذلك إن عملية استخدام الفضاء الإلكتروني في عمليات الإرهاب أو كساحة لعمليات عدائية من شأنها أن تؤثر على الحقوق التي تعد من ضمن ركائز حقوق الإنسان الدولية، حيث تؤدي عملية الاستخدام غير السلمي للفضاء الالكتروني إلى الترهيب وبث الخوف في نفوس السكان ، وكذلك تعرض معلوماتهم للسرقة وانتهاك الخصوصية ، كما أن تعرض الخدمات التي يمكن إن تتاح من خلال الإنترنت كالحكومة الالكترونية يمثل حرماناً للمواطنين أو المدنيين من ممارسة حياتهم بحرية وسلام وممارسة الإرهاب عليهم.

وأن التهديد المختلف الذي تمثله هجمات الإرهاب الإلكتروني يعكس دور الفاعلين من غير الدول في ظل بيئة قانونية مختلفة، فهناك نقصاً في عملية تصنيفات الصراع والعمل على خلق ظروف يمكن من خلالها أن يتم تطبيق القانون الجنائي والنزاع المسلح بصورة شاملة عليها، وهذا التطبيق سيؤثر على تطبيق قانون حقوق الإنسان والذي يرتبط بصورة اكبر بالقانون الإنساني الذي يتم تطبيقه في حالة النزاع المسلح والاتفاقيات الخاصة بحقوق المدنيين تحت الاحتلال، وتأتي اتفاقيات حقوق الإنسان بصورة عامه بعدم فرض حقوق أو واجبات على الأفراد، وما يحمل ذلك من إلزام للدول في حماية تلك الحقوق في كل الأوقات. وعلى العكس من ذلك فان القانون الدولي الإنساني هدف إلى حماية أفراد مجموعات محددة في أنماط محددة للصراع المسلح وهذا ما يشمل الصراعات الخاصة بالحرب الأهلية، أو الصراع ما بين الدول أو الصراعات المسلحة غير الدولية والصراعات المسلحة الدولية، وقد عملت الاتفاقيات والمواثيق الدولية، كاتفاقية لاهاي لعام ١٩٠٧ واتفاقيات جينيف لعام ١٩٤٩ والبروتوكولات الإضافية لعام ١٩٧٧ على حماية حقوق جماعات فرعية محددة والتي تضم المقاتلين والمدنيين من غير المحاربين. ولذا فان القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان قد أتيا في إطار وبيئة مختلفة والتي يمكن أن يتم من خلال الجمع فيما بينهما باستنباط إطار قانوني يتعامل مع هجمات الفضاء الإلكتروني بشكل يجعل هناك توازنا في المسئولية بين الدولة والفرد والجماعات، على أساس من القيم الأساسية التي تتعلق بالعمل على احترام القيم الإنسانية.

## المطلب الثاني:

## الإرهاب الالكتروني والجدل ما بين الأمن والحرية

أوجد الفضاء الالكتروني حقوقا رقمية توازي تلك المادية التي عمل على حمايتها القانون الدولي لحقوق الإنسان وأخذت تلك الحقوق الرقمية في الظهور مع انتشار تكنولوجيا الاتصال والمعلومات وتحول الفضاء الإلكتروني إلى ساحة للتعبير عن الرأي والتعبير، وظهر هناك نمط أخر للحقوق يرتبط بظهور حقوق ترتبط بتلك التكنولوجيا الجديدة كالحق في الخصوصية وفي الوصول إلى المعلومات وفي الحق في التعبير و في الدخول إلى وسائل الاتصالات والحق الشخصي الذاتي في الاتصال والحق في الدخول إلى المعلومات، و الحق في المشاركة الاتصالية وغيرها من الحقوق الرقمية ذات الصلة بحقوق الإنسان. ومن ثم فان استخدام هجمات الإرهاب الالكتروني يعد انتهاكا لتلك الحقوق وأخذت حريات التعبير في الظهور عالميا بشكل مختلف من خلال عملية انتهاكها الواسع حتى من قبل الدول التي

كانت تصنف على أنها منبراً للديمقراطية بعد أحداث ١١ سبتمبر٢٠٠١، وانطلاق الحملة الأمريكية فيما عرف بـ "الحرب على الإرهاب"، ويبدأ يطفو على السطح العلاقة ما بين الأمن والحرية، و إذا كنا عاجزين عن معرفة عدد ضحايا الإرهاب وردود الفعل علية حيث كونها مواجهه بين فعل ورد فعل، فإننا لا نتردد في إحصاء و معرفه الضحية والتي هي الحرية فمع كل عملية إرهابية وكل خطوه من الحرب على الإرهاب تتقلص في المقابل الحريات الشخصية حيث زيادة سطوة العامل الأمني ورجاله على العامل القانوني حين تكمن حقوق الإنسان، ولا يختلف في ذلك كون تلك الحكومات ديمقراطية أو ديكتاتورية فالانتهاك شمل الجميع.

وكما أصبحت تكنولوجيا الاتصال أداة للتعبير والحرية إلا أنها أصبحت عرضة أيضا للانتهاك من قبل ما يسمى بالمجتمعات الديمقراطية والنظم السلطوية على حد سواء مع اختلاف درجات السيطرة، فالدول المتقدمة تتحكم وتسيطر في تدفق المعلومات والاتصال والإعلام والإنترنت على النطاق العالمي في حين تمارس النظم السلطوية رقابة داخلية مزدوجة على شعوبها، وأصبح العالم أمام مثلث المال والتكنولوجيا والسياسة كل منها يؤثر في الأخر وتؤثر نتيجة التفاعل بينهم بالتبعية على مجمل الأوضاع الاقتصادية والاجتماعية والثقافية الدولية .

ويعتبر الفضاء الالكتروني بأوجهه العديدة التجسيد الأفضل للأفكار الديمقراطية ولحرية التعبير والاتصال المفتوح والساحة المفتوحة لعرض الأفكار، التي لا تتماثل مع أي ساحة وجدت من قبل. ولكن لسوء الحظ، فإن الحرية التي قدمتها الإنترنت حساسة للاستخدام السيئ من قبل دول وأفراد وجماعات هم أنفسهم عادة ما يكونون أعداء لحرية الفكر والتعبير. و لكن إذا ما حدث خوف من تأثير ما يتم عرضه علي الفضاء الالكتروني فإن أي رد فعل تجاهها، سيدفع إلي تقليص حرية الاستخدام وسيمثل ذلك نصرا لتلك الجماعات وغيرها وضربة للقيم الديمقراطية ولقد استغل السياسيون الخوف من الإرهاب في تمرير تشريعات تحد من الحقوق والحريات الفردية، وتم استخدام التقنيات المتقدمة لمراقبة وبحث وتتبع وتحليل الاتصالات يحمل معه أخطارا أخري تتعلق بانتهاك حقوق الإنسان، ملازمة فعلي الرغم من أن هذه التقنيات قد تكون مفيدة للغاية في تتبع تحركات ذلك التنظيم وجمع معلومات عنه، إلا أن الحكومات والمؤسسات السلطوية، تستغلها كأدوات تنتهك بها الحريات المدنية بالداخل والخارج وتقليص حرية تدفق المعلومات وتقيد حرية التعبير. ففي الوقت الذي يرى فيه البعض ضرورة التنازل عن بعض الحريات الشخصية لصالح حماية المجتمع وصون حرياته.

ويرى البعض الأخر إن الحريات الشخصية هي جزء لا يتجزأ من منظومة القيم الديمقراطية التي لا يمكن التنازل عنها أو جزء منها، فالحرية والأمن كلاهما يشكل الأخر ويؤثر فيه، فبدون الحرية لا يتحقق الأمن والسلام الاجتماعي وبدون الأمن تصبح الحرية والديمقراطية بلا معنى، لكن عندما تتعارض عمليه الحفاظ على الأمن مع الحرية بحجة الدفاع عن الحرية حينئذ تصبح الحرية كلمة تستغل وتنتهك وتفقد معناها وما يزيد الأمر خطورة عندما تكون المواجهة عالمية والتهديد عالمياً والفاعلون من غير الدول.، ومن ثم يجب أن يتمتع الفضاء الالكتروني بحرية التعبير والرأي والحصول على المعلومات حتى يتم عزل الأفكار المتطرفة ومنعها من تضخيم حجمها وحجم المؤيدين لها، فالتقييد والرقابة علي

الرغم من الحاجة إليها في بعض الحالات التي تشكل تهديدا لأمن الفضاء الالكتروني إلا إن ظرفية ومشروطة ذلك قد ترتبط بأهداف سياسية دون غيرها. وقد تطور هذا الموقف بعد تفجيرات لندن في ٧ يوليو ٢٠٠٥، وأدت الهجمات التي ضربت العاصمة البريطانية إلى إحراز تقدم في المناقشات التقنية حول توحيد المعايير الأوروبية في مجال توثيق المكالمات الهاتفية النقالة والمعلومات على شبكة الإنترنت[1]. وسنت المملكة المتحدة قوانين وتشريعات تمنع المواقع الأصولية كأحد أساليب مكافحة الإرهاب، ويبقي عدد من الإشكاليات يتعلق أهمها فيما بين الحق في الخصوصية والحقوق الرقمية مقابل الأخرى المادية و حرية التعبير والتي جاءت عملية انتهاكها رقميا امتدادا لتراجعها واقعيا تحت مظلة الهاجس الأمني، وبما يتطلب مواجهه شاملة لكل الأبعاد التي تحيط بالظاهرة من بعد ثقافي وقيمي واقتصادي واجتماعي وكون المواجهة يجب إن تكون شاملة وليست فقط أمنية مع تعاظم دور القوة اللينة مقابل الأخرى الصلبة ويكون هناك آثار طويلة المدى صعبة ومدمرة للقيم الديمقراطية، وتضيف ثمنا باهظا فيما يتعلق بتدمير الحريات المدنية بالقياس للضريبة المرتفعة للإرهاب ذاته.[2]

وأصبحت عملية مواجهه الإرهاب الإلكتروني تتطلب التوفيق ما بين الحرية والمصالح الفردية والحقوق السياسية من جانب أخر، وكذلك ما بين الأمن الاقتصادي والأمن القومي من جهة أخرى، فمن احد حقوق الإنسان التي ترتبط بهجمات الفضاء الإلكتروني وحرب المعلومات؛ تتعلق بالخصوصية المادية الطبيعية وخصوصية المعلومات الشخصية والاتصالات وحرية التعبير وعدم الخضوع للرقابة وهذا ما يحتاج إلى التمازج ما بين الحريات السياسية والفردية، ومن جهة أخرى المصالح الاقتصادية والأمن القومي. وجاءت القمة العالمية لمجتمع المعلومات التي عقدت في تونس في دورتها الثانية عام ٢٠٠٥ [3] والتي أكدت الطابع العالمي لجميع حقوق الإنسان والحريات الأساسية وعدم قابليتها للتجزؤ، وترابطها وتآزرها، بما فيها الحق في التنمية، وفقاً لما يجسده إعلان المبادئ بالتأكيد على أهمية الديمقراطية والتنمية المستدامة واحترام حقوق الإنسان والحريات الأساسية، والإدارة الرشيدة على جميع المستويات، والتأكيد على تصميم المجتمع الدولي على تعزيز احترام سيادة القانون في الأمور الدولية والوطنية على السواء ونؤكد من جديد على الفقرات 4 و5 و55 من إعلان مبادئ جنيف ويعترف بأن حرية التعبير وحرية تدفق المعلومات والمعارف والأفكار أساسية في مجتمع المعلومات، وأن هذه الحريات تعود بالنفع على التنمية.[4] وأن يتم التعامل مع الفضاء الإلكتروني وفق القيم الأخلاقية والمبادئ القانونية الموجودة في مختلف الأدوات الدولية، مثل حرية التعبير ووصول الجميع إلى المعلومات والمعرفة، وحماية الحياة الخاصة وحماية الملكية الفكرية والتنوع الثقافي واللغوي؛[5]

---

(1) - جريدة الشرق الأوسط ٧ أكتوبر ٢٠٠٥،

(2) عادل عبد الصادق "المتطرفون وحرية التعبير على الإنترنت بين الأمن والانفتاح "، صفحة قضايا إستراتيجية، جريدة الأهرام، ٢١ فبراير ٢٠٠٥ .

(3) كانت القمة قد تم الاتفاق على عقدها بناء على قرار اتخذته الجمعية العامة للأمم المتحدة في ديسمبر ٢٠٠١ و٢٠٠٢.

(4) للمزيد حول أهداف القمة وميادنها واطر عملها يمكن الدخول إلى موقع الأمم المتحدة على الرابط التالي: (http://www.un.org/arabic/conferences/wsis)

(5) تيريزا فرنتس كماتشو(محرر)؛ محمد أمين السلطي، (مترجم)، **الأبعاد الدولية لقانون المجال السيبرني**، سلسلة اليونسكو، 2002، ص ص٣٠- ٣٣٠.

# الفصل الخامس:

---

# الجهود الدولية في تأمين الاستخدام السلمي للفضاء الالكتروني

---

# الفصل الخامس:
# الجهود الدولية في تامين الاستخدام السلمي للفضاء الالكتروني

انقسمت الجهود الدولية في مكافحة الإرهاب الالكتروني: إلى عده أنماط النمط الأول يتعلق بالعمل على إدخال تلك الجرائم ضمن الجرائم الالكترونية والعمل على إصدار تشريعات وطنية تكافح تلك الظاهرة، أما النمط الثاني : هو سعى عدد من الدول أو التكتلات الإقليمية إلى التعاون فيما بينها في مكافحه الإرهاب والجريمة عبر الانترنت ، أما النمط الثالث : العمل على حث الأمم المتحدة إلى القيام بدور في المكافحة عن طريق فرض سيطرتها على إدارة الانترنت وإقرار ثقافة عالمية للأمن الالكتروني وجاء ذلك عبر تناول ثلاثة مباحث الأول يتناول دور الأمم المتحدة في دعم الاستخدام السلمي للفضاء الالكتروني، وفي المبحث الثاني يتناول جهود ومبادرات الفاعلين داخل مجتمع المعلومات العالمي ، وأما المبحث الثالث فيتناول : نحو ميثاق دولي وثقافة عالمية لحماية الفضاء الالكتروني

## المبحث الأول:
## الأمم المتحدة و دعم الاستخدام السلمي للفضاء الالكتروني

تدفع طبيعة خطر الإرهاب الالكتروني الدولية وتعدد الفاعلين وتنامي درجات الخطر إلى الحاجة إلى دور الأمم المتحدة عبر منظماتها وجهودها لما تتمتع به لدرجة ما بمصداقية في مجال تعزيز التعاون الدولي ، ومن اجل ذلك تناول الباحث ذلك عبر تناول في المطلب الأول: الأمم المتحدة وتنمية الوعي العالمي بالأمن الالكتروني، وفي المطلب الثاني: القمة العالمية لمجتمع المعلومات وإدارة الانترنت.وأما المطلب الثالث: الاتحاد الدولي للاتصالات والمبادرة الخاصة بالأمن الالكتروني

### المطلب الأول:
### الأمم المتحدة وتنمية الوعي العالمي بالأمن الالكتروني

في ظل اهتمام الأمم المتحدة والجمعية العامة بقرارها الخاص بان التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي تتضمن تهديدات محتملة وقائمة في مجال الأمن الالكتروني الذي يتطلب الاهتمام الدولي والعمل على أعاده تعيين المفاهيم الدولية كما جاء ذلك ضمن الدورتين الخاصتين بالقمة العالمية لمجتمع المعلومات والتي عقدت دورتها الأولى في جينيف عام ٢٠٠٣ والثانية في تونس ٢٠٠٥ والتي تعد من انجح الجهود الدولية التي عقدت برعاية الأمم المتحدة.[1]

وتم إنجاز جهود أخرى من المجلس الاقتصادي والاجتماعي للأمم المتحدة ولجنة العلوم والتكنولوجيا من اجل التنمية ومنظمة الأمم المتحدة للتجارة والتنمية ومنظمة الأمم المتحدة للبحث والتدريب، وقامت الجمعية العامة للأمم المتحدة بإنشاء مجموعه عمل خاصة حول امن المعلومات بهدف تنسيق خطة العمل للتنمية العالمية لمجتمع المعلومات مع الأمم المتحدة،و ومن ثم فانه يمكن القول أن ميثاق الأمم المتحدة أن لم ينص صراحة على تجريم استخدام حرب المعلومات كأداة إرهابية أو ما يعرف بالإرهاب الإلكتروني فان روح الميثاق تتفق مع تجريم استخدامه باعتباره يمثل انتهاكاً لما ورد في الميثاق بخصوص " التهديد أو استخدام القوة ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة " مع الأخذ في الاعتبار إن الميثاق جاء لمواجهه النزاعات المسلحة، فانه إذا ما تم اعتبار الإرهاب الإلكتروني واستخدام حرب المعلومات تقع ضمن العدوان والذي يعني يحمل وإرغام دولة على الإتيان بعمل معين فانه تنطبق هنا قوة القانون.

ومن ثم فان ذلك يعني إن النظرة للإرهاب الالكتروني وحرب المعلومات تقع ضمن ميثاق ومقاصد الأمم المتحدة، كما ورد في الفصل السابع من ميثاق الأمم المتحدة فيما يتخذ من الأعمال في حالات تهديد السلم والإخلال به ووقوع العدوان في المادة ٣٩ "يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملاً من أعمال العدوان، ويقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير طبقاً لأحكام المادتين ٤١ و٤٢ لحفظ السلم والأمن الدولي أو إعادته إلى نصابه"[2]. وأورد ميثاق الأمم المتحدة في

---

[1] Henning Wegener , " Harnessing the perils in cyberspace: who is in charge?", Disarmament fourm , icts and international security , three ,2007, pp 46-52.

[2] المادة ٣٩ من الفصل السابع من ميثاق الامم المتحدة.

مادته الثانية فقرة (٣) بان "يفض جميع أعضاء الهيئة منازعاتهم الدولية بالوسائل السلمية على وجه لا يجعل السلم والأمن والعدل الدولي عرضة للخطر"[1]

ومن ثم فان التجاء الدول إلى تسوية منازعاتها وصراعاتها عبر الفضاء الإلكتروني يعرض الأمن والسلم الدولي للخطر والطابع السلمي للعلاقات الدولية، وعنيت الأمم المتحدة بوضع إستراتيجية لمواجهة الإرهاب بمقتضي القرار الذي اتخذته جمعيتها العمومية في ٨ سبتمبر سنة٢٠٠٦ وملحق هذا القرار الذي يتضمن خطة العمل. ويعتبر هذا القرار علامة فارقة سجلت لأول مرة موافقة جميع الدول علي وضع إستراتيجية لمكافحة الإرهاب، وتمثل هذه الإستراتيجية الإطار العالمي الأول لمواجهة الإرهاب، وقد دعت هذه الإستراتيجية الدول الأعضاء للعمل مع نظام الأمم المتحدة لتطبيق خطة العمل التي تتضمنها الإستراتيجية، وقد أدمجت هذه الإستراتيجية معايير حكم القانون عند تنفيذ وثائق الأمم المتحدة المتعلقة بالإرهاب.

وقد أنشئت في نطاق الأمم المتحدة لجنة لمواجهة الإرهابCounterterrorism Committee بعد احداث ١١ سبتمبر ٢٠٠١ طلبت من مكتب الأمم المتحدة للمخدرات والجريمة في فيينا وضع إرشادات للدول عند تشريع وتطبيق وسائل محاربة الإرهاب.. وتنفيذا لذلك وضع المكتب سنة٢٠٠٦ قائمة بالإرشادات تضمنت أربعة أقسام: الأول في الأعمال المجرمة، والثاني في الوسائل التي تضمن التجريم الفعال، والثالث في القانون الإجرائي، والرابع في وسائل التعاون الدولي في المسائل الجنائية، ووضع المكتب في نهاية الإرشادات مشروع قانون ضد الإرهاب.

و أصدرت الأمم المتحدة عبر جمعيتها العامة عدداً من القرارات التي توضح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات استخداما غير سلميا، وجاء ذلك عبر سلسلة من القرارات، والتي منها قرار الجمعية العامة في الدورة ٥٥ /٢٨في ديسمبر ٢٠٠٠ والدورة ١٩/٥٦ في ١٩ ديسمبر ٢٠٠١ بشان إرساء الأساس القانوني لمكافحة إساءة استعمال تكنولوجيا الاتصال والمعلومات في إعمال إجرامية. وجاءت القرارات في الدورة ٥٣ /٧٠في ٤ ديسمبر ١٩٩٨ وفي الدورة ٥٤ /٤٩في ١ ديسمبر ١٩٩٩، والدورة ٢٨/٥٥ ٢٠ نوفمبر ٢٠٠٠، و الدورة ٥٦ /١٩ في ٢٩ نوفمبر ٢٠٠١، والدورة ٥٧ /٥٣ في ٢٢ نوفمبر٢٠٠٢ بشان التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي .

وركزت تلك القرارات على دور العلم والتكنولوجيا في سياق الأمن الدولي وان التطورات العلمية والتكنولوجية يمكن أن تكون لها تطبيقات مدنية وعسكرية على السواء، وبأنه يلزم مواصلة وتشجيع التقدم المحرز في تسخير العلم والتكنولوجيا لأغراض التطبيقات المدنية، ودعا القرار الدول للمزيد من النظر في الأخطار القائمة والمحتملة في ميدان أمن المعلومات، وكذلك فيما يمكن اتخاذه من تدابير للحد من المخاطر التي تبرز في هذا الميدان، وبما يتمشى وضرورة المحافظة على التدفق الحر للمعلومات؛ كما دعا القرار إلى دراسة المفاهيم الدولية ذات الصلة التي تهدف إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية؛ كما يدعو القرار جميع الدول لمواصلة موافاة الأمين العام بتقييمها لمسائل امن المعلومات وتعريف المفاهيم الأساسية المتصلة بأمن المعلومات، والدعوة إلى دراسة الأخطار

[1] الماده ٢فقرة ٣ من الفصل الاول لميثاق الامم المتحدة.

القائمة والمحتملة في مجال أمن المعلومات والتدابير التعاونية التي يمكن اتخاذها للتصدي لها، والعمل على تشكيل فريق من الخبراء الحكوميين.[1]

بالإضافة إلى قرار الجمعية العامة للأمم المتحدة في الدورة ٥٧ /٢٣٩ في ٢٠ ديسمبر ٢٠٠٢ بشأن إرساء ثقافة عالمية لأمن الفضاء الإلكتروني، و٧٣/٥٥ في ٤ ديسمبر ٢٠٠٠ و١٢١/٥٦ ١٩ديسمبر ٢٠٠١، والدورة ٥٨ /١٩٩ في ٢٣ديسمبر ٢٠٠٣، جاء قرار الجمعية العامة للأمم المتحدة بإرساء ثقافة عالمية للأمن الالكتروني وهو يعد من القرارات الهامة التي استهدفت العمل على حماية البنية التحتية الحيوية للمعلومات وحث وتفعيل دور المنظمات الدولية ذات الصلة، ودعوة الدول إلى وضع استراتيجيات لتقليل حجم التعرض للإخطار التي تهديدا للبنية التحتية الحيوية للمعلومات [2]، واتخذت الجمعية العامة للأمم المتحدة في الدورة ٢٥٨/٥٦ في ٣١ يناير ٢٠٠٢ قراراً يدعو إلى استخدام تكنولوجيا الاتصال والمعلومات من اجل التنمية [3].

هذا بالإضافة إلى قرارين صدرا من الجمعية العامة للأمم المتحدة بالدعوة إلى القمة العالمية لمجتمع المعلومات في دورتها ٥٦ في ٣١ يناير ٢٠٠٢ والدورة ٥٧ في ٣١ يناير ٢٠٠٣ [4]، ، وقدمت روسيا في ديسمبر ١٩٩٨ اقتراحا للجمعية العامة للأمم المتحدة طالبت فيه بوضع مسودة قرار يتعلق بأمن المعلومات وحمل القرار مسمى " التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي " وتبنتها بالإجماع الجمعية العامة للأمم المتحدة [5]. ودعا القرار أعضاء الأمم المتحدة لترسيخ التعاون الثنائي والمتعدد الإطراف والأخذ في الاعتبار الأخطار المحتملة والقائمة في مجال امن المعلومات، ودعي القرار أيضا كل الدول لإبلاغ الأمين العام للأمم المتحدة بوجهات نظرهم حول تحديد الأفكار الأساسية المرتبطة بقضايا أمن المعلومات والعمل على تطوير المبادئ الدولية التي من شانها دعم امن نظم المعلومات والاتصالات الدولية والمساعدة في مكافحة الاستخدام الإرهابي والإجرامي لها [6].

وعكس قرار الجمعية العامة للأمم المتحدة الإدراك الكبير لمشكلات امن المعلومات الدولية، وتمت لأول مرة الإشارة إلى الاستخدام العسكري المحتمل لتكنولوجيا الاتصال والمعلومات في القرار المقدم في ١ ديسمبر ١٩٩٩، وتبنت الأمم المتحدة اقتراحاً روسياً في مايو ٢٠٠٠يدعو إلى "تحديد المفاهيم الدولية المرتبطة بأمن المعلومات والتي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية [7]، وفي عام ٢٠٠١ وافق أعضاء الأمم المتحدة على إنشاء "مجموعه الخبراء الحكومية GGE التي بدأت عملها في عام ٢٠٠٤ بهدف مناقشة الأخطار القائمة والمحتملة في مجال امن المعلومات الدولي والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية امن نظم الاتصالات والمعلومات العالمية [8].

---

(1) قرار الجمعيه العامة للامم المتحدة في الدورة ٥٧ /٥٣ ، الصادرفي ٢٢ نوفمبر ٢٠٠١ .
(2) قرار الجميعه العامة للامم المتحدة ١٩٩/٥٨ المؤرخ في ٢٣ ديسمبر ٢٠٠٣.
(3) قرار الجمعية العامة للامم المتحدة في الدورة ٥٦ /٢٥٨ الذي تم اتخاذه في ٤ ابريل ٢٠٠٢.
(4) للمزيد حول وثائق القمة العالمية لمجتمع المعلومات والبيان الختامي لها والاعمال التحضيرية يمكن الرجوع الى الرابط التالي (http://www.un.org/arabic/conferences/wsis/docs.htm)
(5) General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/53/70, 4 January 1999.
(6) Anatolij A Streltsov," International Information Security: Description and Legal Aspects",ICTs and International Security , United Nations Institute for Disarmament Research (UNIDIR), Geneva, 2007 pp5-14.
(7) General Assembly, **Developments in the Field of Information and Telecommunications in the Context of International Security,** UN document A/RES/56/19, 7 January 2002.
(8) Ibid.

وتعد تلك أول مرة يتم اتخاذ قرار سياسي على المستوى الدولي لترجمة الجهود الدولية إلى خطوات عملية، وفي ابريل ٢٠٠٣ قدمت روسيا مبادرة جديدة خاصة للأمم المتحدة تحت عنوان " القضايا المتعلقة بعمل مجموعه الخبراء الحكومية حول امن المعلومات "، كما قدمت روسيا للجمعية العامة قرارا سعى إلى تطوير اتفاقيات الحد من التسلح لكي تشمل عمليات المعلومات أو عمليات شبكات المعلومات، وحملت مسودة القرار الروسي في الدورة ٧٠/٥٣ للجمعية العامة للأمم المتحدة دعوة الدول الأعضاء "لدعم اتجاهات الأخذ في الاعتبار الأطر القائمة والمحتملة في مجال امن المعلومات، والتقدم في مجال تنمية المبادئ الدولي التي يمكن أن تدعم امن نظم المعلومات والاتصالات العالمية والمساعدة في مكافحة الإرهاب المعلوماتي والجريمة، وأشار القرار الروسي إلى أهمية إدراك أن استخدام أسلحة المعلومات ضد البنية التحتية الحيوية يأتي مشابها بنتائج استخدام أسلحة الدمار الشامل ".

وبدأت مسالة دور عمليات المعلومات في الحرب الحديثة يدخل دائرة اهتمام الجيوش الحديثة، وظهرت الحاجة إلى دعم التعاون المتعدد الأطراف والقبول بالمواثيق القانونية الدولية بهدف تقوية الميثاق العالمي لنظام امن المعلومات الدولي، ولكن على الرغم من اجتماع مجموعه الخبراء التي شكلتها الأمم المتحدة في عامي ٢٠٠٤ و٢٠٠٥ بهدف وضع ترتيبات لمسودة قرار يقدم للاماته العامة للأمم المتحدة وعلى الرغم من تنفيذ بعض النجاحات إلا أنها فشلت في التوصل إلى مسودة للقرار واصطدمت بإشكالية إذا ما كان القانون الدولي الإنساني أو القانون الدولي تحديدا يمكنه إن ينظم الإبعاد الأمنية للعلاقات الدولية في حالة الاستخدام العدائي لتكنولوجيا الاتصال والمعلومات عن طريق توظيفها للأغراض العسكرية والسياسية، ومن ثم أصبح عمل مجموعه الخبراء الحكومية الدولية بلا جدوى على الرغم من نجاحها بداية في رفع حالة الوعي بأمن المعلومات على الأجندة الدولية، وقد قررت الجمعية العامة للأمم المتحدة استمرار جهودها لدراسة هذه المشكلة والعمل على إنشاء مجموعه خبراء تبدأ عملها في عام ٢٠٠٩.[1]

وشكل الأمين العام للأمم المتحدة "كوفي عنان" في بداية عام ٢٠٠٤ فريقا دوليا لدراسة قضية إدارة الإنترنت وقد انتهى فريق العمل إلى إيجاد أربعة تصورات، يمثل التصور الأول في إقامة مجلس عالمي للإنترنت يتألف من أعضاء الحكومات ويوفر تمثيلا مناسبا عن كل منطقة ويكون له علاقة بمؤسسات الإنترنت وربطه بالأمم المتحدة، وأن يكون للقطاع الحكومي دور قيادي وللقطاع الخاص والمدني دور استشاري. والتصور الثاني تمثل في توسيع دور اللجنة الاستشارية الحكومية لهيئة الإنترنت.

ودعا التصور الثالث إلى تشكيل مجلس دولي للإنترنت ينهض فيما يتعلق بالسياسات التي تمس المصالح الوطنية للدول عبر الوظائف الموازية لاختصاص هيئة الإنترنت. أما التصور الرابع فقد اقترح إقامة ثلاثة كيانات مؤسسية عالمية لمعالجة إدارة ورسم السياسات والإشراف على الهيئة والتنسيق العالمي. هذه التصورات الأربعة عكست رغبة ضمنية في التخفيف من سطوة الولايات المتحدة على عمل الشبكة، والتي أصبحت وسيلة لا غنى عنها للعالم كله. وتسيطر الولايات المتحدة على النظام الذي يوزع أسماء المواقع ونطاق عملها والشفرة الرقمية التي توصل أجهزة الكمبيوتر إليها عبر برامج متخصصة، وتتمسك منظمة (الإيكان) ICANN الأمريكية التي تتبع وزارة التجارة الأمريكية بهذا الحق بصورة حصرية لعملية إدارة

---

[1] General Assembly, **Developments in the Field of Information and Telecommunications in the Context of InternationalSecurity,** UN document A/RES/61/54, 19 December 2006.

الشبكة ومراقبتها، وهو موقف تراه كثير من الدول غير عادل، ومن ثم تنادى بنوع من الإدارة المشتركة للشبكة بما يجعلها غير مرهونة بدولة بعينها، وإنما بمجموع إرادات الدول المستخدمة لها، مع المشاركة في وضع المعايير التي تحدد الإباحة والحظر في استخدام الشبكة ومدى حقوق الأفراد والجماعات في الوصول إلى مصادر المعلومات وفى تداولها، خاصة مع شيوع ما يسمى بضرورات الأمن مقابل اعتبارات الحرية.

وتعد سيطرة الولايات المتحدة على عمل الشبكة الدولية مبعث قلق للعديد من الدول في العالم، خاصة الدول النامية والتي طالبت بنصيب في هذه الإدارة وحتى قبل قمة جنيف ٢٠٠٣، غير أن الموقف الأوروبي لم يكن متحمسا لهذا المطلب في ذلك الوقت. ومع تغير الموقف الأوروبي ناحية دعم ومساندة مطلب الدول النامية حدث تحول مهم، إذ بدا أن مطلب إنهاء السيطرة الأمريكية أكثر شيوعا من قبل، لاسيما مع مناداة دول الاتحاد الأوروبي بانتخاب هيئة دولية لإدارة الشبكة والرقابة عليها، خاصة بعد تفجيرات لندن في ٧ يوليو ٢٠٠٧، حيث سعت بريطانيا إلى إصدار قوانين تراقب استخدام الإنترنت تم تضمينها في قوانين مكافحة الإرهاب.

وإلى جانب المواقف الحكومية، أخذ العديد من منظمات المجتمع المدني الدولي في ممارسة الضغوط في سبيل إنهاء السيطرة الأمريكية على الإنترنت، باعتبارها تمثل تهديدا للحقوق الرقمية والتي من ضمنها الحق في تداول ونقل المعلومات وحرية التعبير والمشاركة الاتصالية وحرية الاختيار والدخول والحق في الخصوصية، والتي تم تضمينها في التشريعات الإنسانية الكبرى مثل الإعلان العالمي لحقوق الإنسان والميثاق الدولي للحقوق المدنية والسياسية واتفاقية الحقوق والحريات الأمريكية والميثاق الأفريقي لحقوق الإنسان والشعوب والاتفاقية الأوروبية لحماية حقوق الإنسان وحرياته الأساسية، بالإضافة إلى العديد من المواثيق والدساتير الإقليمية. (1)

وعلى مدار عشر سنوات أصبحت الأبعاد المختلفة لقضية امن المعلومات تدخل ضمن اهتمام العديد من المنظمات والمنتديات الدولية والإقليمية مثل الاتحاد الدولي للاتصالات والقمة العالمية للمعلومات ومجلس أوربا بالإضافة إلى الخطى الحثيثة التي اتخذتها الجمعية العامة للأمم المتحدة لدعم إنشاء ثقافة عالمية لأمن الفضاء الإلكتروني وحماية البنية التحتية الحيوية وأثارت الجمعية العامة للأمم المتحدة قضايا أخرى متعلقة بتكنولوجيا الاتصال والمعلومات مثل العمل على إنشاء ثقافة عالمية للأمن الالكتروني وحماية البنية التحتية الحيوية (2) ، وأصبحت قضية امن المعلومات مرتبطة بحظر استخدام تكنولوجيا الاتصال والمعلومات للتأثير أو الهجوم على وسائل تكنولوجيا الاتصال والمعلومات الخاصة بدولة أخرى ،وأصبح الاستخدام العدائي لتكنولوجيا الاتصال والمعلومات يعمل على إنشاء مواقف تشكل تهديدا للسلم والأمن الدوليين.

---

(1) عادل عبد الصادق،" قمة تونس العالمية للمعلومات: استمرار الوضع الراهن !"، مجلة تعليقات مصرية (الكترونيه )، مركز الدراسات السياسية والاستراتيجية بالاهرام، العدد ٤٤ ،٢٢ نوفمبر ٢٠٠٥ يمكن الإطلاع على الرابط التالي(أخر زيارة ٣-٢-٢٠٠٧) (www.ahram.rg.eg/acpss/Ahram\2005\11\22\COMM0.HTM)

(2) See for example, General Assembly, **Creation of a Global Culture of Cybersecurity**, UN document A/RES/57/239,31, See also, January 2003; and General Assembly, **Creation of a Global Culture of Cybersecurity and the protection of critical information infrastructures**, UN document A/RES/58/199, 30 January 2004.

وفيما يتعلق بالإرهاب الإلكتروني تحديدا فان أول تصريح رسمي جاء في رسالة أمين عام الأمم الهذا يجعلي عنان في رسالته في ١٥ مايو ٢٠٠٦ جاء فيه "في عالم يتزايد فيه الترابط وإقامة الشبكات، أضحى من الهام للغاية ضمان سلامة نظمنا وهياكلنا التحتية الحيوية من هجمات مجرمي الفضاء الإلكتروني، والعمل في الوقت نفسه على بث الثقة في التعاملات الالكترونية وغيرها من الخدمات والتطبيقات الالكترونية الأخرى.".

وارتكز موقف الأمم المتحدة عبر أمينها العام على انه طالما يتوقف الأمر على الممارسات الأمنية، التي يتبعها كل من البلدان والشركات والمواطنين المرتبطين بالشبكات فان هذا يجعل من الخطر ذو طابع دولي وما يتطلبه من إرساء ثقافة عالمية لأمن الفضاء الإلكتروني. وطالب أمين عام الأمم المتحدة الدول الأعضاء وأصحاب المصلحة للمساعدة في زيادة الوعي العالمي بأمن الفضاء الإلكتروني وإنشاء شبكة دولية للمبادرات والتدابير المضادة القائمة على تكنولوجيا المعلومات والاتصالات لتعزيز الأمن وبناء الثقة في استعمال تكنولوجيات المعلومات والاتصالات، وأكد الأمين العام أن هذا الأمر أساسي لاستمرار نمو الاقتصاد الدولي وتطوره ويكتسب أهمية خاصة بالنسبة للبلدان النامية[1]

وتتضمن أهداف الأمم المتحدة العمل على حفظ الأمن والسلم الدوليين ولتحقيق ذلك يجب العمل على اتخاذ خطوات جماعية فعالة للقضاء على الأخطار المهددة للسلم والعمل على حل المنازعات بالطرق السلمية، وكذلك العمل على تنمية العلاقات الودية بين الدول التي يكون أساسها احترام الحقوق المتساوية وحق البقاء لجميع الشعوب، و العمل على تحقيق التعاون الدولي في حل المنازعات الدولية ذات الإبعاد الاقتصادية والاجتماعية والثقافية أو الإنسانية و نص ميثاق الأمم المتحدة في المادة ٤٣ فقرة (١) من الفصل السابع بان " يتعهد جميع أعضاء "الأمم المتحدة" في سبيل المساهمة في حفظ السلم والأمن الدولي، أن يضعوا تحت تصرف مجلس الأمن بناء على طلبه وطبقاً لاتفاق أو اتفاقات خاصة ما يلزم من القوات المسلحة والمساعدات والتسهيلات الضرورية لحفظ السلم والأمن الدولي ومن ذلك حق المرور" ويمكن أن نشير إلى ما ورد في عبارة "المساعدات و التسهيلات الضرورية"، وكل ما تراه الأمم المتحدة يخدم الأمن الدولي ويساعد في ترسيخه من قبيل شبكات وتكنولوجيا الاتصال والمعلومات التي قد تكون هامة إما في سبيل دعم وحفظ الأمن الدولي أو في طابعها الدولي وارتباطها وأهميتها الدولية والتي قد تغري احد أطراف النزاع على استخدامه. ومن ثم فان الأمم المتحدة أصبحت بحاجة إلى العمل على تحييد الفضاء الإلكتروني، ووضع القواعد المتعلقة بهذا المجال وتطبيقها وإقرار النظام العام والمحافظة على السلم والأمن الدوليين ويتطلب ذلك تنازلات من الدول المتقدمة وخاصة الولايات المتحدة التي ما زالت تحتكر إدارة الإنترنت والعمل على الموزانة بين حق الدول في استخدام الفضاء الإلكتروني وفي نفس الوقت توفير الحماية من الأخطار التي تهدده.

وظهرت معوقات الأمن الجماعي التي تتمثل في عدم استكمال البناء المؤسس لنظام الأمن الجماعي، واستحالة استخدام الترتيبات المؤقتة المنصوص عليها في المادة ١٠٦ والتي تسمح للدول الموقعة على إعلان

---

(1) كان ذلك في رسالة الامين العام "كوفي عنان " بمناسبة توقيع مدير عام المنظمة الإسلامية للتربية والثقافة والعلوم (إيسيسكو)، عبد العزيز عثمان التويجري، ومدير عام منظمة التربية والعلم والثقافة (يونسكو)، كويشيرو ماتسورا، في ١٥ مايو ٢٠٠٦ في باريس، برنامج تعاون جديد لعامي ٢٠٠٦-٢٠٠٧. للمزيد يمكن الاطلاع على الرابط التالي (اخر زيارة ٢٣-٩-٢٠٠٨)
(http://www.un.org/arabic/news/fullstorynews.asp?newsID=5690)

موسكو بالإضافة إلى فرنسا باتخاذ إجراء جماعي باسم الأمم المتحدة للمحافظة على السلم والأمن الدوليين لان هذه الدول هي نفسها الدول الدائمة العضوية في مجلس الأمن "، وتحدي تفعيل دور مجلس الأمن ليمارس صلاحياته في حل المنازعات بطرق سلمية وكذلك في قمع العدوان وفقاً للفصل السابع من الميثاق. ويتطلب تفعيل دور الأمم المتحدة في إحكام الفوضى داخل الفضاء الإلكتروني إطاراً قانونياً يحكمه وينظم استخدامه [1] والعمل على دعم الأمن الجماعي الدولي، واتخاذ ما يعرف بـ " التدابير المضادة " وهي "تدابير سلمية غير مصحوبة باستعمال القوة العسكرية وتتمثل في عدم امتثال دولة أو عده دول لواحد أو أكثر من التزاماتها الدولية التي تتحملها في مواجهه دولة أخرى رداً على ارتكابها عملا غير مشروع دوليا بهدف حملها على العودة للامتثال لالتزاماتها القانونية "[2]

وتم استحداث منصب رئيس مكافحة الإرهاب الجديد في الأمم المتحدة و مساعد الأمين العام ومنوط به تعزيز القدرة على مكافحة الإرهاب بين الدول الأعضاء، وتشجيع التعاون بشأن الإجراءات التي يقررها مجلس الأمن.[3] وهناك ثلاثة محاور تضمن فاعلية التعاون الدولي، وإن كانت هناك معوقات لهذا التعاون في المرحلة الحالية بحسب ترتيب الأولويات فقد نجحت البرامج الجديدة التي أعدتها الأمم المتحدة في التغلب على هذه المشكلات والمعوقات، كما نجحت في وضع معايير الأولويات، وكان أهمها تعزيز العمل الأمني الدولي؛ لتحقيق أقصى درجات الفاعلية، ووضع الأدلة العلمية في خريطة يُستدل بها على طبيعة الجريمة ومداها واتجاهاتها. وسعت الأمم المتحدة للتوعية بشان مخاطر استخدام شبكة الإنترنت في الأعمال الإرهابية والتي تقود المنظمة العالمية حملة توعية في إنحاء العالم ضد التشدد، الذي يلقى مساعدة من الإنترنت، وذلك عن طريق التعليم في المدارس ووكالات الأمم المتحدة مثل منظمة التربية والعلوم والثقافة التابعة للأمم المتحدة "اليونسكو".

## المطلب الثاني:
## القمة العالمية لمجتمع المعلومات وإدارة الإنترنت

تميزت قمة تونس ٢٠٠٥ تميزت بسيطرة موضوع إدارة شبكة الإنترنت على جدول أعمالها، وذلك لتحولها من البعد التقني والفني إلى أن تصبح ذات بعد سياسي واجتماعي وفي إطار محاولة صياغة الحقوق الرقمية وبلورتها سياسيا وقانونيا مقابل الأخرى المادية. وجاء بالإضافة إلى ذلك ثلاث قضايا أخرى هي قضية تمويل مشروعات الاتصالات والمعلومات التي تسد الفجوة الرقمية بين دول الشمال والجنوب، ووجوب استخدام مؤشرات لقياس التقدم والنمو في الاتصالات والمعلومات بالدول النامية وقياس الفجوة الرقمية، ووضوح المحتوى الرقمي وتحديات تحقيق هذا المحتوى على الصعيد التعليمي والثقافي والاقتصادي والاجتماعي، وبحث القمة الإعداد لما بعد قمة تونس.

---

(1) David G. Post," Against “**Against Cyber Anarchy**” Berkeley university,US,vol.7, ,2002 .
( http://www.law.berkeley.edu/journals/btlj/articles/vol17/Post.stripped.pdf)

(2) للمزيد حول شروط التدابير المضادة وعناصرها واهميتها في تعزيز الأمن الجماعي انظر : د.عابدين عبد الحميد حسن قنديل ،" التدابير المضاده في النظام القانوني الدولي :دراسة نظرية وتطبيقية "، رسالة دكتوراة غير منشورة ، كلية الاقتصاد والعلوم السياسية ، جامعه القاهرة ص ص ٤٢٧-٤٣٣ .

(3) جريدة الشرق الأوسط "الأمم المتحدة:الإنترنت سهلت عمل الجهاديين ويجب مراقبتها "١٤-١١-٢٠٠٧

واتفقت جميع الحكومات في المرحلة الأولى للقمة العالمية في ديسمبر 2003 على أن: "السلطة السياسية على قضايا السياسات العامة المتصلة بالإنترنت تعتبر حقاً سيادياً للدول. إذ تملك حقوقاً ومسؤوليات بشأن قضايا السياسات العامة الدولية المتصلة بالإنترنت" وطالبت حكومات الدول الأمين العام للأمم المتحدة بضرورة البحث في مسألة إدارة الإنترنت بدءا من (صياغة تعريف لهذه العبارة) كنقطة انطلاق للبحث في غير ذلك من الموضوعات. فمسائل مثل ICANN ونظام نطاق الأسماء DNS وبصفة خاصة نطاق الأسماء المتعلق بالدول ccTLD Names ونظام الخادم الجذري أو الأساسي Root Server System[1] ونظام اللغة المستخدم في نطاق الأسماء...الخ كانت كلها مسائل شائكة في قمة جنيف أمام الجميع[2].

وفى مواجهة الضغوط الدولية لجعل الإنترنت يخضع إدارته للأمم المتحدة تمسك الموقف الامريكى بالسيطرة على عمل الشبكة وإدارتها، واعتبر إن هذه السيطرة التقنية ليست ضد انتشار الإنترنت أو حرية استخدامها من قبل اى جهة كانت. ويركز الموقف الأمريكي على أنه يدعم جهود الأمم المتحدة لكي تصبح كل الشعوب على خريطة المعلوماتية، وان كل دولة تتحكم في الإنترنت الداخل إليها والخارج منها، كما توجد هيئات ومنظمات تدير بعض جوانب الإنترنت.

وتمر مسارات المعلومات عبر الولايات المتحدة دون أن تقوم واشنطن بأية سلطة على هذه المعلومات، لان دورها هو جانب فني تنظيمي. وأن مسألة احتكار الولايات المتحدة للكود التقني المحدد لمسارات الإشارات الرقمية يرجع لكون الولايات المتحدة تاريخيا هي مخترعه الإنترنت، ومن ثم يصبح لها حق الملكية الفكرية، وان منظمة الايكان هي صاحبة الحق في إدارة الإنترنت وهي جهة غير هادفة للربح ولها مجلس إدارة عالمي لا يضم سوى عدد قليل من الأمريكيين ورئيسها استرالي. كما ترى الولايات المتحدة انه لا يمكنها أن تضحى بسيطرتها على عملية تنظيم أسماء المواقع على الشبكة لجهاز بيروقراطي مجهول. وطرحت الدول النامية مطلبها بالمشاركة في إدارة الإنترنت لم تكن على أتم الاستعداد سواء من الناحية الفنية أو السياسية. والمرجح أنها كانت تهدف إلى الضغط على الولايات المتحدة وحلفائها لتوفير التمويل اللازم لصندوق التضامن الرقمي الذي عهدت به قمة جنيف على اثر اقتراح الرئيس السنغالي.

وترى الدول النامية أن الإنترنت أصبحت مرفقاً عالمياً وليس خاصا بالولايات المتحدة، وأنها من أهم الركائز الأساسية لإقامة مجتمع المعلومات على المستوى القطري أو الإقليمي أو العالمي، وبالتالي هناك أهمية قصوى لمناقشة وضبط الطريقة التي تدار بها الشبكة والجهة التي تسيطر عليها، وان منظمة الإيكان لا تخضع لأية اتفاقيات دولية تتعلق بسياسة إدارة الإنترنت مما يعني أن تكون عرضة لقرارات تعسفية أحادية الجانب بدون أن يكون لأي دولة حق الرفض، وان ترك الوضع على ما هو عليه سيضع في يد الولايات المتحدة أوراق ضغط إضافية على العالم ربما تتطور إلى إجراءات قد تضر بالآخرين، وان كل من يسيطر على كل أو جزء من هذه النظم يمكنه استغلالها كوسيلة للتربح المادي بلا حدود ويمارس نوعا

---

(1) هناك ١٣ خادم جذري حتى الأن، ١٠ منها موجود في الولايات المتحدة لاسباب تاريخية ليس الا. وهي مثار جدل حتى في مسألة تعريفها وتحديد خصائصها العالمية والاقليمية على السواء. خاصة وان مطلب الدول في قمة جنيف الاولى كان توفير مسيرات خوادم اقليمية!! ولن تقم الدول بتحديد تعريف للخادم الجذري الاقليمي او الدولي. ومع ذلك فإنه قبل انعقاد القمة تم استخدام نظام استنساخ الخوادم الجذرية حول العالم، فاضحى هناك أكثر من خادم يحوي ذات ما هو موجود في الخوادم الـ ١٣ المذكورة. لذلك فالاعتقاد السائد الان أن ما تردد في اعلان المباديء في قمة جنيف هو تكرار وتحصيل حاصل.

(2) Adam Peake, **Internet governance and the World Summit on the Information Society (WSIS)- Prepared for the Association for Progressive Communications** (APC) June 2004 P. 3.

من الاحتكار والابتزاز.[1] وترى الدول النامية أن سيطرة أي طرف على إدارة الإنترنت بدون ضوابط يجعلها عرضة للتلصص والتجسس، ومن ذلك المحاولات التي تم اتخاذها للحد من حرية التعبير على شبكة الإنترنت بدعوى مكافحة الإرهاب، وان كان ذلك الانتهاك لا يأتي بمعزل عن ما أصاب الحريات المدنية بعد هجمات ١١ سبتمبر، حيث أخذت شكل إجراءات رسمية حكومية علنية، بعد أن كانت مثل هذه الإجراءات محصورة في أعمال أجهزة الاستخبارات وحسب. وعلى الرغم من المساعي الدولية لسحب الرقابة الأمريكية على شبكة الإنترنت فانه كانت هناك جهودا دولية لإخضاع الشبكة الدولية للمعلومات لرقابة الأمم المتحدة، وان كان هذا المسعى قد واجه بعض الصعوبات التي تتمثل في تشدد الإدارة الأمريكية في موقفها.[2]

وشكل الأمين العام للأمم المتحدة فريق عمل معني بإدارة الإنترنت وكان من مهام هذا الفريق (صياغة تعريف عملي لإدارة الإنترنت) وفي منتصف يونيو ٢٠٠٥ قدم التعريف التالي " إدارة الإنترنت تعني قيام الحكومات والقطاع الخاص والمجتمع المدني، كل حسب دوره، بوضع وتطبيق مبادئ ومعايير وقواعد وإجراءات لصنع القرار وبرامج مشتركة تشكل مسار تطور الإنترنت واستخدامه". ووفقا لهذا التعريف فقد تم حصر مؤسسة ICANN في إطار نطاق الأسماء وبالتالي لا تهمين على إدارة الإنترنت وإنما أشرك التقرير الحكومات والقطاع الخاص والمجتمع المدني في هذا الإطار وبما يعني بقاء الحال على ما هو عليه.[3]

وفيما يتعلق بالسياسة العامة والإشراف على الصعيد العالمي، خلص فالعمل إلى إلى أنه ينبغي لأي شكل تنظيمي لمهمة الإدارة/مهمة الإشراف أن يتمسك بالمبادئ التالية :أنه "لا يجوز لحكومة واحدة أن تستحوذ على دور غالب في مجال الإدارة الدولية للإنترنت.وان يتخذ الشكل التنظيمي لمهمة الإدارة طابع التعددية اللغوية والشفافية والديمقراطية مع مشاركة كاملة من جانب الحكومات والقطاع الخاص والمجتمع المدني والمنظمات الدولية. أن يفسح الشكل التنظيمي لمهمة الإدارة مجال المشاركة أمام جميع أصحاب المصلحة والمنظمات الحكومية الدولية والمنظمات الدولية ذات الصلة، كل في نطاق دوره."واتفق الفريق على أن التدويل المتواصل للإنترنت ومبدأ العالمية يؤكدان كلاهما ضرورة إعادة النظر في آليات الإدارة الحالية.

وتمَّ استعراض نماذج تنظيمية مختلفة لهذا الغرض، ووقع الاختيار على أربعة نماذج لكي تكون موضوعاً للبحث والنظر وشملت هذه الخيارات سيناريوهات مختلفة يدعو بعضها إلى مزيد من التدويل للإشراف على الإنترنت، مع تعزيز المشاركة الحكومية، لاسيما ما يخص مسائل السياسة العامة، وفقاً لما تنشده بلدان كثيرة، أو إنجاز ذلك في سياق الهياكل القائمة، كما تحبذ الولايات المتحدة وبعض الحكومات الأخرى. ولم يقترح أي من هذه الخيارات أن تتولى الأمم المتحدة دور الهيئات التقنية المعنية بإدارة موارد الإنترنت، ولم يؤيد أي منها إنشاء وكالة جديدة تابعة للأمم المتحدة؛ بل إن بعضها لم يشر قط إلى دور للأمم المتحدة.[4] وأوصى الفريق أيضاً بإنشاء فضاء أو "منتدى" جديد للحوار يمكن لجميع أصحاب

---

[1] عادل عبد الصادق، " قمة تونس العالمية للمعلومات: استمرار الوضع الراهن، مرجع سابق ذكرة

[2] Charles E. Jr. Croom, Guarding Cyberspace: Global Network Operations. Joint Force Quarterly No. 46, 2007.pp 68-69

[3] المزيد حول هذا الموضوع يمكن الاطلاع على وثائق القمة العالمية لمجتمع المعلومات في دورتيها الاولى والثانية على الموقع التالي (: http://www.un.org/arabic/conferences/wsis) أخر زيارة (١٧-١١-٢٠٠٨ )

[4] عادل عبد الصادق ،" قمة تونس العالمية للمعلومات: استمرار الوضع الراهن، مرجع سابق ذكرة

المصلحة الالتقاء في إطاره على قدم المساواة لمناقشة القضايا ذات الصلة بإدارة الإنترنت. ولن يكون لهذا المنتدى أي صلاحيات فيما يتعلق بصنع القرار. اعترفت عملية القمة بأن الإنترنت التي تعتبر عنصراً مركزياً في البنى التحتية لمجتمع المعلومات قد تطورت من مرفق للبحث والدراسات الأكاديمية إلى مرفق عالمي متاح للجمهور عامة. وأصبح الفضاء الالكتروني وسيلة عالمية هامة للاتصالات والتجارة، وتكتسب أهمية فائقة للشعوب والحكومات في البلدان كافة، كما يتزايد دورها الحيوي في مجال الأمن القومي وتباينت وجهات النظر تتباين بشكل أساسي فيما يتعلق بمفهوم مهمة "الإشراف" وترتيباتها العملية، ومثال ذلك: ودعا المقترح الأرجنتيني إلى "تعزيز دور الحكومات في عملية صنع القرار داخل مؤسسة الإنترنت للأسماء والأرقام المخصصة فيما يتعلق بقضايا السياسة العامة ذات الصلة بالإنترنت". وهذا يوحي بضرورة تعزيز دور اللجنة الاستشارية الحكومية التابعة لتلك المؤسسة.

ودعا الاتحاد الأوروبي إلى صوغ "نموذج جديد للتعاون الدولي"، يتركز فيه دور الحكومات على "القضايا المبدئية للسياسة العامة، بمنأى عن المشاركة في العمليات اليومية العادية" بينما ترى المجموعة العربية، بعد استعراضها للنماذج الأربعة المقدمة في تقرير فريق العمل، أن إنشاء مجلس عالمي للإنترنت هو أفضل وسيلة لتناول موضوع السياسة العامة والإشراف. وتقترح جمهورية إيران الإسلامية إقامة "مجلس دولي حكومي للسياسة العامة والإشراف على الصعيد الدولي". وعندما صدر كل من إعلان المبادئ وخطة العمل عن قمة جنيف تضمن كل منهما مسألة الإقرار بحاجة الإنترنت إلى إدارة:

و جاء في إعلان المبادئ (البند ٤٨- وقد تطورت الإنترنت لتصبح مرفقا عالميا متاحا للعامة وينبغي أن تشكل إدارتها قضية مركزية في جدول أعمال مجتمع المعلومات. وينبغي أن تكون الإدارة الدولية للانترنت متعددة الأطراف وشفافة وديمقراطية، وبمشاركة كاملة من الحكومات والقطاع الخاص والمجتمع المدني والمنظمات الدولية. ويجب أن تكفل توزيعا منصفا للموارد وأن تيسر النفاذ أمام الجميع وان تكفل تشغيلا مستقرا وآمنا للانترنت مع اعتبار تعدد اللغات)، كما جاء في (البند ٤٩ – تنطوي إدارة الإنترنت على قضايا تقنية وقضايا تتعلق بالسياسات العامة على حد سواء، وينبغي أن يشترك فيها جميع أصحاب المصلحة والمنظمات الدولية الحكومية والمنظمات الدولية ذات الصلة.

وكان من أهم نتائج القمة العالمية لمجتمع المعلومات التي عقدت في تونس ٢٠٠٥ العمل على إيجاد مدخل رعاية صحية تفاعلي لتبادل البيانات بين البلدان المنخفضة الدخل والعالية الدخل ووضع نظم للتنبؤ بالكوارث الطبيعية والكوارث الناجمة عن النشاط البشري، ورصد التأثيرات البيئية وتطوير مشاريع للتخلص الآمن بيئيا من معدات الحاسوب وإعادة تصنيعها، وإقامة شراكات لتبادل المعلومات بشأن الزراعة ومصائد الأسماك والغابات، ووضع إجراءات وقائية للأمن الحاسوبي بالتركيز على المصارف لإجراء معاملات موثوق بها مباشرة على الإنترنت وتشجيع البلدان على صياغة تشريعات أمنية تتعلق بتكنولوجيا المعلومات، وإقامة جهاز اتصال لمعالجة الحوادث والاستجابة لها في الوقت الحقيقي، ووضع شبكة تعاونية لتبادل المعلومات [1]

---

(1) للمزيد حول إعلان القمة يمكن الإطلاع على موقع القمة على الانترنت على العنوان التالي:
(www.un.org/arabic/conferences/wsis)

## المطلب الثالث:

## مبادرة الاتحاد الدولي للاتصالات للأمن الالكتروني:

كان قانون الاتصالات قد طرأ علية العديد من التطورات عبر الزمن منذ بدايته بهدف حماية الكابلات البحرية، وليصبح الآن قانون اتصالات حديث تحت قيادة الاتحاد الدولي للاتصالات، والتي تحولت لمنظمة متخصصة في تكنولوجيا المعلومات والاتصال (١)، وتنص المادة ٣٥ من ميثاق الاتحاد الدولي للاتصالات على عملية التدخل في عمل الاتصالات. وجاء في الإعلان الخاص بالقمة العالمية لمجتمع المعلومات " بناء الثقة والأمن في استخدام تكنولوجيا الاتصال والمعلومات " وتولى الاتحاد الدولي للاتصالات القيام بهذه المهمة وانطلاقا من ذلك قام الاتحاد الدولي بدعم التعاون ما بين الشركات الخاصة والقطاع العام من أجل تنسيق الجهود والعمل على تبني إستراتيجية عالمية للأمن الالكتروني، وإنشاء بوابة الكترونية للأمن الالكتروني.

وأصبح الاتحاد الدولي الاتصالات بمثابة ملتقي دولي رئيسي لهذه الأنشطة، كما قام الاتحاد الدولي بالتعاون مع مجلس أوربا الذي أنجز الاتفاقية الأوروبية حول الجريمة الالكترونية من أجل الاستعانة بها في عملية وضع إطار قانوني دولي، وكذلك التعاون مع الاتحاد الأوروبي ومنظمة الأمن والتعاون في أوروبا ومكتب الأمم المتحدة لمكافحة الجريمة والمخدرات كذلك مع الانتربول الدولي والايروبول الخاص بالاتحاد الأوروبي، وتسعى تلك الجهود في إطار تنفيذ الأجندة العالمية للأمن الالكتروني. تم عقد المؤتمر الإقليمي حول الأمن الالكتروني بالتعاون مع الاتحاد الدولي للاتصال في قطر في فبراير عام ٢٠٠٨ والذي جاء ضمن إحدى توصيات إعلان الدوحة الصادر عن المؤتمر العالمي لتنمية الاتصالات المنعقد بالدوحة في مارس ٢٠٠٦. وقد اعتمد المؤتمر آنذاك ما يسمى بـ "خطة عمل الدوحة"، ويقوم فريق عمل رسمي من الإتحاد الدولي للاتصالات بتطوير "تقرير حول أفضل الممارسات لمنهج وطني للتعامل مع قضايا الأمن الالكتروني."(٢)

وتم التأكيد على وضع إستراتيجية وطنية لأمن الالكتروني وإقامة تعاون بين الحكومة والصناعة، ومواجهه الجريمة الالكترونية، واستحداث مقدرة وطنية لإدارة الحوادث، ودعم الثقة في الأمن الالكتروني. واقر المؤتمر دعوة جميع الدول بوضع وتنفيذ إطار وطني للأمن الالكتروني وحماية البنية التحتية الحرجة للمعلومات والتي تعد بمثابة خطوة أولي في سبيل التصدي للتحديات التي تواجهها جراء اتصالها بتكنولوجيا المعلومات والاتصال.(٣)

وكان تأمين الشبكات من أهم نتائج القمة العالمية لمجتمع المعلومات وتم تعيين الاتحاد الدولي للاتصالات بوصفه الميسِّر الوحيد لخط العمل (ج ٥)، "بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات". وقد هيأ النمو السريع لشبكات تكنولوجيا المعلومات والاتصالات فرصاً جديدة للمجرمين لاستغلال مواطن الضعف في النفاذ الإلكتروني ومهاجمة البني التحتية الحساسة للبلدان. ونتيجة لتزايد التهديدات بشكل مثل خطر يهدد مستقبل نمو مجتمع المعلومات العالمي. وعلاوة على ذلك، فإن الفضاء الإلكتروني لا حدود له: ويمكن للهجمات الالكترونية أن تلحق أضراراً هائلة في بلدان متعددة وفي غضون

---

(1) See ITU website: http://www.itu.int/net/about/index.aspx. Last visited: Feb. 24, 2008.

(2) المجلس الأعلى للاتصالات وتكنولوجيا المعلومات في قطر يمكن زيارة موقعه على الانترنت على العنوان التالي
(http://www.ict.gov.qa/output/Page635.asp)

(3) للمزيد حول الاعلان الختامي للمؤتمر يمكن الاطلاع علية على الرابط التالي (اخر زيارة ١٢-٤-٢٠٠٨)
(http://www.ituarabic.org/2008/CIIP/Doha_Declaration.pdf)

دقائق معدودات.[1] و تعتمد الحكومات والمؤسسات والأفراد بصورة متزايدة على المعلومات المخزونة والتي يجري نقلها عبر شبكات الاتصالات المتقدمة. والتكاليف المرتبطة بالهجمات السيبرانية تكون باهظة بالفعل - من حيث الخسارة في الإيرادات، وفقد البيانات الحساسة، والأضرار التي تلحق بالمعدات، وتعطيل الخدمات، وتوقف الشبكات عن العمل، ويعمل الاتحاد الدولي للاتصالات جاهداً من أجل التصدي للتحديات الناشئة المرتبطة بمجتمع المعلومات. ويتصدى عمل الاتحاد في مجال التقييس بصورة مباشرة لمواطن الضعف المتعلقة بأمن الشبكات وقدرات الإرسال.

ويكفل وضع المعايير مستويات محددة للأداء والأمن في مجالات التكنولوجيات والأنظمة والمنتجات، على نحو يعزز الثقة بين موفري الخدمات والمستعملين النهائيين. وتغطي المعايير الأمنية للاتحاد طائفة عريضة من المجالات، بما في ذلك المبادئ الأمنية لشبكات الاتصالات المتنقلة الدولية من الجيل، وأنظمة الوسائط المتعددة باستعمال بروتوكول الإنترنت، وشبكات الجيل التالي،(IMT3G) الثالث والشروط الأمنية للشبكات، واقتحام الشبكات، والسرقة ومنع الخدمة، وسرقة الهوية، والتلصص، والاستدلال البيولوجي عن بُعد من أجل استيقان وأمن اتصالات الطوارئ. وقد مكّنت أعمال الاتحاد في مجال التصديق الإلكتروني الولايات القضائية حول العالم من الاعتراف بوثائق البريد الإلكتروني باعتبارها مستندات قانونية، ومن منح التوقيعات الإلكترونية صفة قانونية.

وينفرد قطاع تقييس الاتصالات في الاتحاد بوضع يهيئ له أن يجمع بين القطاع الخاص والحكومات لتنسيق الأعمال في مجال مواءمة السياسات الأمنية العامة والمعايير الأمنية حول العالم. ويعمل الاتحاد بصورة وثيقة مع المنظمات الأخرى المعنية بوضع المعايير المتعلقة بالأمن ورصد الأعمال المضطلع بها في مجال الأمن، كما يستضيف ورشة عمل مشتركة تعقد بصورة منتظمة لتنسيق الأعمال بين مختلف المنظمات الأخرى المعنية بوضع المعايير. ويقوم الاتحاد، بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات، وفريق التوجيه المعني بأمن الشبكات والمعلومات، بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات، التي تسلّط الضوء على المعايير الحالية، والأعمال الجارية، والمعايير المتوخاة في المستقبل فيما بين المنظمات الرئيسية المعنية .

وتشارك لجان الدراسات التابعة للاتحاد في العديد من الأنشطة المتصلة بالأمن، ويعد استعراض القضايا الأمنية جزءاً رئيسياً من أعمالها. وأقرت لجنة الدراسات الرئيسية المعنية بأمن نظام الاتصالات ما يربو على مائة توصية بشأن أمن الاتصالات، وبخاصة في سلسلة سواء بمفردها أو بالاشتراك مع المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية / التوصيات الدولية). وتنشر بانتظام دليلاً أمنياً بشأن "الأمن في تكنولوجيا المعلومات والاتصالات" يعد بمثابة استعراض عام للمسائل الأمنية وتوصيات قطاع تقييس الاتصالات بالاتحاد من أجل تأمين الاتصالات (وقد صدرت النسخة الثالثة من هذا الدليل في أغسطس ٢٠٠٦ )، علاوة على خلاصة أمنية تتضمن قائمة بالتوصيات التي أقرّها قطاع تقييس الاتصالات بالاتحاد فيما يتصل بأمن الاتصالات. ويسعى الاتحاد الدولي للاتصالات اللاسلكية ITU الذي يضم ١٩١ دولة التي

---

[1] الاتحاد الدولي للاتصالات - التقرير السنوي للاتحاد، ٢٠٠٧ ، ص - ٣٨ يمكن الإطلاع علية على الرابط التالي (اخر زيارة ٢٣-١٠- ٢٠٠٨ ) (http://www.itu.int/aboutitu/annual_report/2007/pdf/2007-ar.pdf)

تستخدم نظام الهاتف العالمي في أن يأخذ زمام المبادرة للمطالبة بمعاهدة عالمية ضد الجريمة الالكترونية، بالإضافة إلى المبادرات الدولية السابقة.[1] ووضع إطار دولي لتعزيز الأمن الالكتروني - برنامج الأمن السيبراني العالمي وتم تعيين فريق خبراء لإسداء المشورة إلى الأمين العام للاتحاد بشأن المسائل المعقدة التي تكتنف موضوع الأمن السيبراني. ويتألف فريق الخبراء رفيع المستوى من متخصصين مرموقين عالمياً في مجال الأمن السيبراني ومستمدين من خلفية واسعة النطاق تمثل صانعي السياسات، والحكومات، والأوساط الأكاديمية، والقطاع الخاص. وسيقوم الفريق بصياغة المقترحات التي ستُقدَّم إلى الأمين العام للاتحاد بشأن الاستراتيجيات الطويلة الأجل لتعزيز الأمن السيبراني في خمسة مجالات.

وفي إطار مجال العمل المعني "بالتدابير القانونية"، يتم إسداء المشورة بشأن كيفية التعامل مع الأنشطة الإجرامية التي تُرتكب عبر شبكات تكنولوجيا المعلومات والاتصالات من خلال وضع تشريعات بطريقة متوافقة دولياً. أما "التدابير التقنية والإجرائية" فتركز على التدابير الرئيسية الرامية إلى معالجة مواطن الضعف في منتجات البرمجيات، بما في ذلك خطط الاعتماد والبروتوكولات والمعايير. وتضع "الهياكل التنظيمية" إطار العمل واستراتيجيات الاستجابة فيما يتعلق بمنع الهجمات السيبرانية وتتبُّعها والرد عليها وإدارة الأزمات المتعلقة بها، بما في ذلك حماية أنظمة البنية التحتية الحرجة للمعلومات. ويركز مجال "بناء القدرات" على وضع استراتيجيات لآليات بناء القدرات من أجل زيادة الوعي، ونقل الخبرة المتخصصة، وتعزيز الأمن السيبراني في إطار برنامج السياسات العامة الوطنية. ويهدف مجال "التعاون الدولي" إلى وضع إستراتيجية للتعاون والحوار والتنسيق على الصعيد الدولي في مجال التصدي للأخطار الالكترونية. ويشارك الاتحاد أيضاً في تقديم المساعدة التقنية المباشرة من أجل بناء قدرات الدول الأعضاء، ولاسيما البلدان النامية، على تنسيق الاستراتيجيات الوطنية وحماية البني التحتية للشبكات ضد المخاطر. ويلزم وضع أطر عمل واستراتيجيات وطنية تتيح لأصحاب المصلحة استعمال جميع الأدوات التقنية والقانونية والتنظيمية المتاحة في مجال تعزيز ثقافة للأمن الالكتروني.

وفي حين أحرزت بعض البلدان تقدماً في استراتيجياتها الوطنية في مجال الأمن الالكتروني وحماية البنية التحتية الحرجة للمعلومات، بدأ البعض الآخر ينظر فيما يتعيَّن اتخاذه من تدابير. ويعمد قطاع تنمية الاتصالات إلى وضع إطار لتنظيم نهج وطني للأمن السيبراني يحدد الأهداف الرئيسية المتعلقة بالسياسة العامة للاستراتيجيات الوطنية في مجال الأمن السيبراني على النحو التالي: وضع إستراتيجية وطنية للأمن الالكتروني و إقامة تعاون على المستوى الوطني بين الحكومة ودوائر الصناعة، و استحداث قدرة إدارية للتحكم في الحوادث وطنياً و ردع الجريمة الالكترونية، و النهوض بثقافة وطنية للأمن الالكتروني، ويعمل الاتحاد مع الكثير من الشركاء من القطاعين العام والخاص بشأن مبادرات إنمائية محددة في مجال الأمن السيبراني/حماية البنية التحتية الحرجة للمعلومات بغرض مساعدة البلدان النامية في مجالات التوعية، والتقييم الذاتي، وبناء القدرات، وتوسيع نطاق المراقبة، والإنذار، وقدرات الاستجابة للحوادث.

---

[1] وذلك مثل، القوانين الأميركية الفيدرالية الإجرائية بشأن جرائم الكمبيوتر، وقانون إساءة استخدام الكمبيوتر البريطاني، القانون الفرنسي لجرائم الكمبيوتر رقم ١١٧٠ لعام ١٩٩٠،ودليل الأمم المتحدة الإرشادي بشأن الجرائم المرتبطة بالكمبيوتر لعام ١٩٩٤ منقحا ومعدلا كما في عام ٢٠٠١، ومقررات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات ١٩٩٤ البرازيل - ريودي جانيرو بشأن جرائم الكمبيوتر، الاتفاقية العالمية ( الأوروبية ) لجرائم الكمبيوتر لعام ٢٠٠١، قرار مؤتمر الأمم المتحدة بشأن جرائم الكمبيوتر لمنع الجريمة ومعاملة السجناء هافانا ١٩٩٠ - قرار بشأن الجرائم ذات الصلة بالكمبيوتر.

ويشجِّع الاتحاد الدولي للاتصالات على تقاسم الخبرات بين البلدان المتقدمة والبلدان النامية وفي داخل هذه البلدان من خلال برامجه الإلكترونية، وبرنامج جارٍ لورش عمل إضافة إلى توفير مجموعات أدوات. وطالبت القمة العالمية لمجتمع المعلومات في تونس في نوفمبر ٢٠٠٥، وان يقوم الاتحاد الدولي للاتصالات بتنسيق آلية لبناء الثقة والأمن في مجال استخدام تكنولوجيا الاتصال والمعلومات، ويوفر الاتحاد الدولي للاتصالات المنظور العالمي والخبرة المطلوبة لمواجهه التحديات، وقام بإطلاق برنامج الأمن الالكتروني العالمي.

و تحظى الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات بأهمية أساسية في بناء مجتمع معلومات شامل وآمن وعالمي، وللثقة والأمن أهميتها الحيوية في الاستعمال الفعال، وخاصة عندما تتسم التحديات التي تفرضها لها طابع قانوني وتقني ومؤسسي عالمي، وان تلك التحديات لا يمكن مواجهتها إلا في إطار تعاون دولي ومواجهتها على المستوى المحلي والإقليمي، وبرنامج الأمن الالكتروني العالمي (GCA)[1] هو إطار أعده الاتحاد الدولي للاتصالات بهدف اقتراح استراتيجيات للتوصل إلى حلول لتعزيز الثقة والأمن في مجتمع المعلومات وحيث يتم التركيز على المبادرات الوطنية والإقليمية القائمة على تجبن الازدواجية في العمل وتشجيع التعاون فيما بين جميع الشركاء المعنيين. ويقوم المجرمون والإرهابيون والهاكر وغيرهم باستغلال أوجه الضعف والثغرات في التشريعات الوطنية والإقليمية ، وهناك من الدلائل التي تشير إلى أنهم يحولون عملياتهم إلى البلدان التي لا توجد فيها حتى الآن قوانين ملائمة ويمكن تطبيقها حتى يتم لهم شن الهجمات على ضحاياهم في ظل إفلات كامل تقريبا من العقاب أو حتى البلدان التي لديها قوانين بالفعل لم تسلم من التعرض لمثل تلك الاعتداءات. وتوجد خمس ركائز لبرنامج الأمن الالكتروني العالمي للاتحاد الدولي للاتصالات. هي: التدابير القانونية، التدابير التقنية والإجرائية، والهياكل التنظيمية، وبناء القدرات، والتعاون الدولي. ويتألف برنامج الأمن الالكتروني العالمي من سبعه أهداف إستراتيجية هي:

١. وضع استراتيجيات لاستحداث تشريع نموذجي لمكافحة الجريمة الالكترونية يمكن تطبيقه عالميا وقابل للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي
٢. وضع استراتيجيات عالمية لإيجاد الهياكل التنظيمية والسياسات العامة الملائمة على الصعيدين الوطني والإقليمي بشأن الجريمة الالكترونية
٣. وضع إستراتيجية لصوغ معايير أمنية دنيا وخطط اعتماد للأجهزة والبرمجيات والأنظمة تكون مقبولة عالميا
٤. وضع استراتيجيات لإيجاد إطار عالمي للرصد والإنذار والاستجابة للحوادث، لضمان التنسيق عبر الحدود بين المبادرات الجديدة و القائمة.
٥. وضع استراتيجيات عالمية لإنشاء وإقرار نظام هوية رقمية عام عالمي، والهياكل التنظيمية اللازمة لضمان الاعتراف بوثائق التفويض الرقمية عبر الحدود الجغرافية.
٦. وضع استراتيجيات عالمية لبناء القدرات البشرية والمؤسسية من اجل تعزيز المعارف والمهارات
٧. وضع مقترحات بشأن إطار لإستراتيجية عالمية لأصحاب المصلحة المتعددين لتحقيق التعاون والحوار والتنسيق على الصعيد الدولي في جميع المجالات .

---

[1] The Global Cybersecurity Agenda (GCA), A Framework for International Cooperation in Cybersecurity, International Telecommunication Union (ITU),April ,2008.
للمزيد حول استراتيجية الاتحاد يمكن الاطلاع على الرابط التالي (اخر زيارة ٢٤-٨-٢٠٠٨)
(http://www.itu.int/osg/csd/cybersecurity/gca/overview/index.html)

## المبحث الثاني:
## جهود ومبادرات الفاعلين داخل مجتمع المعلومات العالمي

**يتناول هذا المبحث فرص وتحديات تعزيز الأمن الالكتروني الدولي والذي شكل قضية دولية مرشحة للاهتمام المتصاعد في المستقبل مع تعاظم الاعتماد الدولي على تكنولوجيا الاتصال والمعلومات في المرافق الحيوية ويوضح من خلال تناول عدد من النقاط المحورية الهامة التي تتعلق بملامح المجتمع الدولي الحديث ومكونات تبني إستراتيجية للأمن الالكتروني الدولي.ويستعرض الباحث ذلك عبر المطلب الأول: الجهود الدولية في مكافحة الإرهاب الالكتروني ، أما في المطلب الثاني فيتم تناول : المبادرات الدولية لتعزيز امن الفضاء الالكتروني .**

### المطلب الأول:
### الجهود الدولية في مكافحة الإرهاب الالكتروني

أصبح للفضاء الالكتروني دور في كافة مجالات الحياة وجعل من العالم وحدة واحدة وبدأت تظهر الأخطار الالكترونية التي يمكن ان تهدد دوره واهميته الاستراتيجية بعد التغير الرئيسي الذي ظهر في سياسات الأمن بعد انتهاء الحرب الباردة حيث كان للأمن خلال تلك الفترة له مضامين مختلفة وجاءت الثورة التكنولوجية لتضيف إلية أبعاد أخرى جديدة.

ومع نهاية الحرب الباردة لم ينته فقط النظام ثنائي القطبية بل مثل أيضا نهاية الأخطار التقليدية التي ترتبط بالحدود وسيادة الدولة، فمع تفتت الاتحاد السوفيتي برزت أخطار دولية غير عسكرية مثل الهجرة والإرهاب والانتشار النووي بالإضافة إلى أخطار أخرى غير تقليدية والعابرة للحدود الدولية، والتي أصبحت تقع ضمن أولويات أجنده الأمن الدولي .

وفي بداية التسعينات بدأت موجة الانتشار العالمي لتكنولوجيا الاتصال والمعلومات وبدأ مستخدمو تلك الأدوات في الازدياد عالميا وتدخل في كافة مجالات الحياة الاقتصادية والسياسية والاجتماعية والأمنية وفي نفس الوقت تعرضت تلك الأدوات التكنولوجية الجديدة للاستخدام السيئ من قبل الإرهابيين والأخطار الأخرى التي أصبحت تهدد وظيفتها ودورها في خدمة المجتمع الدولي بما فرض ذلك تحديات أمام صانعي القرار، وتتكون عملية المواجهة من عاملين هما الأول بدرجة التنوع في الاستخدام وفي الفاعلين وفي الاستخدام المدني والعسكري، أما العامل الأخر فيتعلق بالقواعد القانونية والثقافية والتقنية التي يمكن أن تشكل نواه لوضع قيود أو استراتيجيات الحماية التي تطبق .

وعلى الرغم من الاعتقاد الشائع بأن الاهتمام بالأمن الالكتروني لم يصبح ظاهرة في التسعينات فإن الفيروسات والديدان أصبحت جزءا من مصادر القلق للأمن الالكتروني من أيامه الأولي حيث ظهرت معالم الخوف من أحداث تعلقت بتمكن احد القراصنة من اختراق الكمبيوتر الخاص بالقيادة والسيطرة للترسانة النووية الأمريكية عام ١٩٨٦ ، وجاءت فيروسات cuckoo egg في منتصف الثمانينات لرفع الوعي بشان الدور الذي يمكن أن يلعبه الكمبيوتر كوسيلة من وسائل التجسس الخارجي والحصول على المعلومات الهامة.

ولكـن مـع بدايـة التـسعينات أصـبحت البيئـة التكنولوجيـة تتـسع مـع انتـشار تكنولوجيـا الاتـصال والمعلومـات وارتباطهـا بالأعمـال والاقتصاد والمجتمـع الـدولي، وفي منتصف التسعينات أصبحت قضية الأمـن الالكتروني تدخل ضمن أجنده الأمـن القـومي مـع ارتباطها بالإرهـاب وحماية البنية التحية، وفي تلك الإثنـاء ظهـرت قطاعـات حديثـة في الاقتصاد تعتمـد علـى تكنولوجيـا الاتصال والمعلومـات اعتمـادا كـبيرا، وأصبح الأمـن الالكترونـي يمثـل عنـصراً هامـا مـن عناصـر الأمـن القـومي واسـتراتجياته، وذلـك لأهميـة الفـضاء الإلكتروني في تطور الاقتصاديات الحديثة والنمو الاقتصادي.

وأصبحت الخطورة لا تكمن فقط في تعرض أنظمة المعلومات للفشل بل أيضا في أنها أصبحت أهدافاً محتملة للتعرض للهجمات التي تؤثر بدورها على عمل البنية التحتية الكونية للمعلومات والخدمات التي تقدمها، ومـا يكـون لـذلك مـن آثار اقتصادية وسياسـية واجتماعيـة وأمنيـة، ومـا يزيـد مـن تلـك المعضلة أن التعـرض للهجمات قد تكـون صـغيرة ورخيصة ولكنهـا تحـدث آثـاراً ضـخمة مـن خـلال شـبكات المعلومـات والاتصال، ولـذا أصبح ذلك التهديد الجديد يستحوذ على اهتمام متزايد من العديد من الدول خاصة تلك التي ترتبط بالتكنولوجيا ومتقدمة صناعيا، ويهتم بها صـانعو القـرار ويقـع ضمن أولويات الأجنـدة الأمنية والسياسية.

وكانـت أول الجهـود الدوليـة الـتي هـدفت لمواجهـه الجريمـة الالكترونيـة والإرهـاب تعـود إلى ثلاثـة عقـود ماضية حين ناقش الانتربول الـدولي إمكانية إيجاد تشريع قـانوني حـول الجريمـة الالكترونيـة في عـام ١٩٨١ [1]. وبـدأ التقـدم بطيئـا ولكنـة اخـذ في التـسارع ببطء بعـد انتهـاء الحـرب البـادرة، ولعـل إنـشاء معهـد قـانون الفضاء الإلكترونـي في جامعة جـورج تـاون الأمريكيـة عـام ١٩٩٥ يـدل علـى نمـط المـشكلة، حيـث يوجـد ثلاثون متخصصاً من الذين يعملون على تحديد كيفية التعامل مع مشكلات الفضاء الإلكتروني، [2]

ويـدأ الخـوف مـن سـقوط الولايـات المتحـدة في أيـدي هـا كـرز وإرهـابيين دولـيين في فـتره الـرئيس بيـل كلينتون، والذي اعتبر إن هجوم حـرب المعلومات يمكـن إن يكـون جـزءا مـن عملية عسكرية تقليدية، أو يمكن للعدو المتوقع استخدام المعلومات كطلقة تحذير لتهديد الولايات المتحدة للعدول عن موقف معين في سياستها الخارجية، أو كجزء من عملية إرهابيه محدودة، ومن النقاط التي وضعت كأهداف محتمله لهذا الخطر نظام الاتصالات أو شبكة الكمبيوتر حيث تعتمد القوات العسكرية الأمريكية على نظم النقل التجارية لنقل الجنود وهـذه النظم تعتمد على شبكات الكمبيوتر للتحكم في الماكينات والتحكم في الاحتيـاط وعملية التنسيق والتمـوين ، وبـذلك يمكـن لجهـة خارجيـة عرقلـه القـوات الأمريكيـة، وكـذلك تعتمـد نظـم الطـوارئ علـى البـرامج الإذاعيـة التجاريـة والإنترنـت الـتي تـساعد في التـسيق والمتابعـة، ويمكـن اسـتهداف نظـم وحواسـب شـركات معينـه لهـا أهميـه خاصـة في إنتـاج الأسـلحة الأمريكيـة أو في حركـه

(1) Stein Schjolberg, Chief Judge, Moss Tingrett Court, Norway. **"Law Comes to Cyberspace," A presentation at the 11th UN Criminal Congress,** Bangkok, Thailand. Workshop 6: Measures to combat computer-related crime. Apr. 18-25, 2007,

(2) د. وليد عبد الحي، " إشكالية الفضاء الإلكتروني في حقوق الملكية الفكرية"، المؤتمر العالمي العلمي الأول حول الملكية الفكرية، جامعة اليرموك، المملكة الأردنية الهاشمية، ١٠-١١ / ٧/ ٢٠٠٠.

التعبئة، وهناك البنوك والمؤسسات المالية التي تكون عرضة للتلاعب بالبيانات المسجلة إما بجمع المعلومات بغرض المساومة أو زرع معلومات خاطئة .(1)

وفي يونيو ١٩٩٧ أصبح ضعف العسكرية الأمريكية في مواجهه هجمات الاتصالات واضحا عندما أطلق قائد القوات المشتركة تدريباً سمى "بالملتقى المناسب" لقياس قدرات الكمبيوتر الدفاعية، وقد اثبت هذا التدريب إن لصوص الكمبيوتر المحترفين أمكنهم تعطيل محولات الطاقة في تسع مدن أمريكية، ومنع خدمات الطوارئ المحلية من الاستجابة لهذه الأزمة، واستغلوا انشغال الحكومة بهذه الإحداث ليتمكنوا من التجول بحرية داخل موقع البنتاجون محدثين الدمار، وتعطيل أوامر القيادات العليا للبنتاجون. وكان أول تحرك في إستراتيجية الدفاع الأمريكية هو قيام الرئيس بيل كلينتون بتكليف الجنرال المتقاعد "روبرت ث مارش" لدراسة التهديدات الخارجية التي تواجه نظم المعلومات و البنية التحتية مثل وسائل النقل ومولدات الطاقة .

وتم الاعتراف بحجم التهديدات التي تواجهه الأمن القومي الأمريكي، وعين" بيل كلينتون" منسقا دوليا لتأمين وحماية البنية التحتية ولمكافحه الإرهاب وفي فبراير ١٩٩٨ قامت وزارة العدل بوضع مركز حماية البنية التحتية تحت تصرف مكتب التحقيقات الفيدرالي لمتابعه أي هجوم على نظم المعلومات ، وفي مارس ١٩٩٨ بدأ البنتاجون في التحري عن أخطر الهجمات على أنظمة الكمبيوتر الأمريكية فيما سمي " متاهة ضوء القمر ".(2)

وقامت مجموعه من لصوص الكمبيوتر باقتحام الشبكات الخاصة بوكالة الفضاء الأمريكية "ناسا " والبنتاجون وهيئات حكومية أخرى وجامعات ومراكز أبحاث وسرقوا آلاف الملفات التي تحتوي على أبحاث فنية وعقود ووسائل إخفاء المعلومات وبيانات غير سرية لكنها جوهرية تتعلق بأنظمة البنتاجون لتخطيط الحروب، ومنذ اكتشاف هذه الواقعة انخرطت هيئة الاستخبارات الأمريكية بأكبر مجال تحقيقي استخباراتي في مجال الاتصالات الالكترونية، وبعد ثلاث سنوات من العمل تم اكتشاف الهجمات بانه تم توجيهها من خلال سبعه مواقع روسية على الإنترنت، وعلية فقد قامت واشنطون بإبلاغ موسكو بهذه النتائج وزودتها بأرقام الهواتف التي صدرت منها هذه الهجمات غير إن الحكومة الروسية قالت إن هذه الأرقام غير موجودة بالخدمة ن وظل الهجوم مستمرا وانشأ هؤلاء اللصوص ما يعرف بالأبواب الخلفية والتي عن طريقها يمكن معاودة الدخول للمواقع التي اقتحموها مسبقا وسرقة بيانات إضافية .

وعلى الرغم من التدمير الذي أحدثته "متاهة ضوء القمر" فإنها لا تعدو أن تكون مجرد بداية للأخطار القديمة، وبدأ القادة العسكريون يدركون أن خسارة المعارك المعلوماتية سيقوض بشكل متزايد قدرة أي دولة على خوض هذا النوع من هذه الحرب – فلن يساوي مشروع الدفاع الصاروخي المليارات التي ستنفق على إقامته إذا ما دمرت الهجمات الرقمية برامجه التكنولوجية وبنيته التحتية، وفي أكتوبر ١٩٩٩ تم البدء في تدريب أخر أطلق علية "نجم القمة" لإجراء تجارب على الدروس المستفادة من تدريب الملتقى المناسب وفي

(1) **Information Security: Emerging Cyber security Issues Threaten Federal Information Systems.** Washington, GAO, May 2005. p72.Report to Congressional Requesters Also available online at: (http://www.au.af.mil/au/awc/awcgate/gao/d05231.pdf)

(2) Arnold K. Veazie, **U.S. Strategy for Cyberspace.** Carlisle Barracks, PA, U.S. Army War College, 2003. p32.Also available online at: ( http://handle.dtic.mil/100.2/ADA416602)

هذا التدريب قام لصوص الإنترنت بمهاجمه أنظمة القوى التي تغذي عددا من القواعد العسكرية الأمريكية وقاموا بإرباك أنظمة الطوارئ في محطات الطاقة السابق ذكرها بسيل من المكالمات عن طريق الكمبيوتر(1).

ودفع ذلك الى انشاء العديد من المبادرات الخاصة من الهيئات التي تقدم تقارير عن تبادل المعلومات والتحذيرات ومراكز داخل الولايات المتحدة وفي الخارج، و قررت الإدارة الأميركية في عهد الرئيس بيل كلينتون إجراء خطوات تنفيذية لمكافحة ظاهرة "الإرهاب الإلكتروني " Cyber terrorism، وبناء عليه تم عام ١٩٩٦ إنشاء "لجنة حماية البنية الحساسة" Commission of critical infrastructure protection. (PCCIP) وأجرت هذه اللجنة سلسلة دراسات وأبحاث تناولت كل النقاط الحساسة في الأمن القومي الأميركي وخصوصاً في مجال التكنولوجيا فوجدت إن المعادلة التي تجمع قطاعات الكهرباء والاتصالات والكومبيوتر هي من الركائز الضرورية لسكان الولايات المتحدة وأمن نظامهم العام وتفوقهم على سائر الأمم.

ورأت اللجنة إن هذه المعادلة: كهرباء + اتصالات + كومبيوتر، معرّضة جدياً لتهديدات "الحرب الرقمية" Cyber-warfare. وأعطت تعريفاً للتهديدات الممكنة ضمن هذا الأسلوب فقالت: "المصادر التي يعتمد عليها من يريد القيام بهجوم رقمي متوافرة ومنتشرة بين عامة الناس وتتألف من جهاز كومبيوتر ونقطة اتصال بالإنترنت وأخذ الاهتمام بالأمن الالكتروني في الانتشار على مستوى العالم وخاصة داخل الدول المتقدمة ، وظهر ذلك في تبني سياسات أمنية متعددة وسعت العديد من دول العالم خلال السنوات القليلة الماضية لزيادة الاهتمام والذي ظهر في عمليات صنع القرار على أعلى مستوى في سبيل الرغبة في تامين نظم المعلومات التي أصبحت تهدد النمو الاقتصادي والأمن القومي حيث أصبحت المخاطر الالكترونية تهدد الظروف المواتية والمشجعة للنمو الاقتصادي وزيادة النسبية الإنتاجية العمل ورأس المال والتي تضمن للأفراد مستوى معيشة مرتفعاً ، ويتحسن باستمرار وتأمين وضع اقتصادي عادل وآمن يشجع الاستثمار الداخلي والخارجي في قطاعات تكنولوجيا الاتصال والمعلومات والاقتصاد الالكتروني الجديد.

واتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني أو الثنائي أو الإقليمي من اجل العمل على حماية البنية التحتية الكونية للمعلومات من خطر التعرض لمثل تلك الأخطار واتجهت الدول لإيجاد اطر تشريعية جديدة تتعامل مع تلك الظاهرة المستحدثة ، والعمل على صياغة مفهوم جديد للأمن القومي، ثم الاتجاه إلى التعاون الدولي من اجل رفع حالة الحماية والتدريب والوعي خاصة مع الطابع الدولي للأخطار الالكترونية التي تتجاوز الحدود التقليدية عبر شبكات الاتصال والمعلومات وأصبح الأمن الالكتروني مندمجاً في البنية التحتية الكونية للمعلومات، وفرض ذلك الحاجة لتحديد ما يمكن أن يمثل بنية تحتية حرجة وتم ذلك من خلال عدد من الإجراءات والسياسات خاصة مع التعامل مع ظاهرة جديدة وتحمل خصائص غير تقليدية (2).

---

(1) James Adams ,virtual defense "Foreign Affairs",vol.80,No.3,may/june 2001,pp 15-18

(2) United States. General Accounting Office. **Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed.** Washington, GAO, 2002. p44 ..
Also available online at: (http://www.gao.gov/new.items/d02918t.pdf)

وحتى منتصف التسعينات كان هناك ثلاثة استراتيجيات لحماية البنية التحتية للمعلومات في الولايات المتحدة كانت تتضمن الفعل العسكري والتدخل والحلول الفنية لتامين الأنظمة "الاستعداد "، وبناء الوعي "المعلومات "، في حين جاءت السياسات الحكومية الخاصة بمكافحة هجمات الفضاء الإلكتروني وتعزيز الأمن الالكتروني متنوعة في مراحل تنفيذها وبعضها كان قويا بينما كانت الأخرى مجرد اقتراحات، والتي جاءت بأشكال وصور متنوعة تراوحت بين أتباع سياسة تنظيمية خاصة بالبنية التحتية للمعلومات لتضمين تلك الإجراءات الخاصة بالأمن الالكتروني في الجهود العامة لمكافحة الإرهاب.

وقد عكست الجهود الدولية في مجال الأمن الالكتروني اهتماماً واضحاً ومتزايداً من جانب القطاع الخاص والعام أو بالتعاون فيما بينهما، وذلك دون التوصل بالضرورة إلى طبيعة المشكلة أو متطلبات حماية الفضاء الإلكتروني، واعتمد هؤلاء الفاعلون على المصادر التي بين أيديهم وجاءت جهودهم تعبيراً عن وجهه نظرهم في المشكلة، وهناك عدد قليل من الدول من انشأ منظمات حكومية تختص بالتعامل مع قضايا الأمن الالكتروني، واتجه اغلب هذه الدول إلي إنشاء العديد من الهيئات والأقسام الحكومية المختلفة .

وسعت العديد من دول العالم المتقدم إلى تبني إستراتيجية قومية في مجال تامين الفضاء الإلكتروني فهناك من الدول من سن وقوانين وتشريعات وطنية وهناك من اتجه إلى تعزيز التعاون الدولي والإقليمي في مجال المكافحة، وتم تضمين خطر التعرض لهجمات الفضاء الإلكتروني ضمن استراتيجيات الأمن القومي، بل اتجه بعض مراكز الأبحاث إلى إنجاز مسودة اتفاق دولي تختص بتامين الفضاء الإلكتروني مثل اقتراح "سيمون جودمان " لإنجاز اتفاق دولي[1] وفي عام ١٩٩٧ قامت مجموعه الثماني الصناعية بإنشاء مجموعه فرعية للجريمة عالية التقنية، وتبنت ما عرف بالمبادئ العشرة " حول مكافحة جرائم الكمبيوتر وأصبح الهدف هو منع الاستخدام الإجرامي للانترنت في إي مكان في العالم .

وفي عام ٢٠٠٠ صدرت مسودة اتفاق عالمي حول الجريمة والإرهاب الإلكتروني من جامعه "استاند فورد "فيما عرف بخطة ستاندفورد وشملت تلك الخطة العديد من النقاط حول هدف الوصول إلى تعاون دولي أوسع في مقاومة هجمات الفضاء الإلكتروني ، وذلك على اعتبار أن الإرهابيين والمجرمين يستغلون نقاط الضعف في القوانين، وخاصة مع التطور المستمر في التكنولوجيا وجمود الأطر القانونية الحالية في مواجهه الأخطار والهجمات ، وفي المادة ١٢ من تلك الخطة تقترح بإقامة وكالة دولية لحماية البنية التحتية الكونية للمعلومات[2]. والعمل على دعم التعاون حول الأمن الالكتروني في كل دول العالم، وقد نبعت روح تلك الاتفاقية من المنظمة الدولة للملاحة الجوية والاتحاد الدولي للاتصالات. كما إن مركز الدفاع الالكتروني الذي أنشاه حلف الناتو ربما يمثل نموذجاً هاماً كمنظمة، وتم إنشاء المركز العالمي للاستجابة

---

(1) Seymour E. Goodman and Herbert S. Lin (eds),"**Toward a Safer and More Secure Cyberspace,** Washington, National Academies Press, 2007. p 307.

(2) وقد تم تكوين تلك المسودة من تسعه خبراء من جامعه ستاندفورد بالولايات المتحدة الأمريكية في عام ٢٠٠٠ وذلك في إطار مؤتمر دولي تم عقده في ديسمبر ١٩٩٩ بجامعه ستاند فورة بدعم من مؤسسة هوفر ،و التجمع من اجل البحث في امن المعلومات والسياسة CRISP ، ومركز الأمن الدولي والتعاونCISAC وجامعه ستاندفورد بالإضافة إلى دعم كل من منظمات المجتمع المدني والشركات ورجال الصناعة والأكاديميين من العديد من دول العالم ، وقد كانت تلك المسودة إضافة هامة للتوصل إلى الاتفاقية الأوروبية للجريمة الالكترونية في نوفمبر ٢٠٠١، للمزيد حول تلك المسودة :
( http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm)

الطوارئ بما يجعله شبيها للمنظمات الدولية الأخرى كالنظام القانوني للجرف القاري في إطار القانون الدولي للبحار "[1].

واخذ الاهتمام العالمي يتزايد بعد ١١ سبتمبر ٢٠٠١ والتي أعقبها التوصل لاتفاقية مجلس أوروبا حول الجريمة الالكترونية في نوفمبر ٢٠٠١ [2]، وبعد أحداث ١١ سبتمبر٢٠٠١ وضع البنتاجون خطة بعنوان " خريطة طريق لعمليات المعلومات "، وهي تستهدف مراقبة الإنترنت والتعامل معها "كمنظومة سلاح معادية "، وفي أكتوبر عام ٢٠٠١ تم عقد اجتماع ضم خبراء التقنية العالية وخبراء العديد من الشركات العاملة في تكنولوجيا المعلومات الأمنية، و قام الرئيس بوش بتعيين ريتشارد كلارك كأول مستشار خاص بالأمن الرقمي وتم إنشاء مكتب الأمن للفضاء الالكتروني، وإدراكاً لأهمية هذا التهديد طلبت الإدارة الامريكيه نحو ٤,٥ بليون دولار لحماية البنية التحتية، وعمل مكتب التحقيقات الفيدرالي على زيادة تحقيقاته حول الأمن المعلوماتي لتصل إلى ما يقرب من الألف تحقيق وتشكيل لجنة متابعه على مدار الساعة.[3]

وقد أدركت الإدارة الأمريكية على نحو فعلي بقدرة تنظيم القاعدة في مجال التكنولوجيا عندما وجدت القوات الأمريكية أجهزه كمبيوتر محمول مع أعضاء تنظيم القاعدة في أفغانستان، وعلى الرغم من عدم استخدام هذه الاجهزه في العمليات الإرهابية بصورة مباشره ولكنها استخدمت في الاتصال والتنسيق للهجمات وتلقي الأوامر وإرسال الرسائل، وأظهر تنظيم القاعدة تطورا بارعا في كيفية استخدام الإنترنت، فكان اكتشاف الرسائل الالكترونية لخالد شيخ محمد هي نقطة البداية للوصول إلى اعتقاله والذي اعتبرته الاستخبارات الأمريكية اكبر عمل في الحرب ضد القاعدة.

وأجرت الولايات المتحدة في يوليو ٢٠٠٢ محاكاة للتعرض لهجوم من الفضاء الإلكتروني سميت "بيرل هاربور الالكتروني، وجاء إنشاء "لجنة حماية البنية الحساسة"، في الولايات المتحدة لتؤسس مجموعه خاصة تتناول جوانب الإرهاب الالكتروني وأطلقت عليها اسم: "مركز حرب المعلومات" الذي يضم نحو ألف موظف وبينهم مجموعة تعمل على مدار الساعة مناوبة للرد على أي تطورات أو استفسارات. وتم إنشاء المركز القومي لحماية البنية التحتيةNIPC ومركز تحليل وتبادل المعلومات ISACs وبرنامج حراسة البنية التحتية INFRAGARD وغيرها من المبادرات وعلى مدار التسعينات أصبح هذا المركز من أهم مراكز حرب المعلومات في النصف الغربي من الكرة الأرضية. إلا أن تطوير المركز واجه عراقيل عديدة أهمها تشابك صلاحيات التحقيق بين CIA ومكتب التحقيقات الفيدرالي (FBI).

هذا بالإضافة إلى مشاريع أخرى مثل "أيشلون" (مقام بالاشتراك مع دول أوروبية للتجسس على رسائل الإنترنت والمكالمات الهاتفية في العالم) وكارنيفور وغيرهما، مع وجود تشابك واضح في الصلاحيات بين تلك الأجهزة.فكان مكتب FBI مكلف بمتابعة التهديدات داخلياً، وكذلك استخبارات الجيش بينما

---

(1) المزيد حول تلك الاتفاقية وبنودها يمكن زيارة موقعها على الإنترنت على الرابط التالي : ( http://www.un.org/Depts/los/index.htm)

(2) للمزيد حول تلك الاتفاقية يمكن الوصل لها بالرابط التالي : www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf

(3) Gabriel Weimann ," Cyber terrorism: How Real Is the Threat?", The United States Institute of Peace,, Special Report No. 119, December 2004.

كانت تعمل CIA في مواجهة القضايا الخارجية. وانتشرت في أجهزة الأمن الامريكيه المختلفة وحدات خاصة بالإرهاب الإلكتروني، وقيام الـ"FBI" بملاحقة المخترقين والقراصنة Hackers على أنواعهم. وتقوم أجهزة الخدمات السرية بملاحقة الإرهاب الإلكتروني في حالات الصرف الآلي والتحويلات المالية عبر الإنترنت والنصب والاحتيال والتصنت، أما سلاح الجو الأمريكي فأسس "فرق هندسة الأمن الالكتروني" ESETs، ومهمتها محاولة اختراق أنظمة وشبكات عسكرية. واستطاعت هذه الفرق اختراق ٣٠٪ من شبكات الأجهزة العسكرية في العالم(1). وظهرت المخاوف من تعرض أنظمة التحكم الإشرافي والحصول على البيانات SCADA للانتهاك عندما تستخدم الإنترنت للمراقبة والتحكم في العمليات الإنتاجية من مواقع بعيدة، والتي تستخدم في مجموعه واسعة من الصناعات، و قامت الولايات المتحدة بإنشاء وزاره الأمن الداخلي في صيف ٢٠٠٣ والتي تركز دورها في الحماية من الأخطار التي تأتي من الجبهة الداخلية وذلك في إطار الحرب على الإرهاب، وأصبحت المخابرات والرقابة عنصرا حيويا في تلك الحرب، ولكن مع تزايد المخاوف الأمريكية من تصاعد التهديدات الالكترونية عالميا.

وجاءت تلك الخطوة ضمن الخوف المتزايد من تعرض البني الحساسة لهجوم الكتروني، وذلك للعمل على إيجاد فرصه لتعزيز الأمن الالكتروني ليكون مستعدا لصد إي هجوم مرتقب من المخترقين والقراصنة والإرهابيين وكذلك ضد المدونات الالكترونية التي تنشر معلومات مزيفة، وأجريت هذه المناورة عبر حواسب أمنة في مركز الخدمة السرية في واشنطون. وظهرت مطالب داخل الولايات المتحدة بعد تولي الرئيس الأمريكي باراك اوباما باستحداث منصب جديد في البيت الأبيض هو مساعد الرئيس لشؤون الانترنت وذلك بعد عجز وزارة الأمن الداخلي عن مواجهه تهديدات الإرهاب الالكتروني (2)

وتقع الولايات المتحدة في عدة إشكاليات للمواجهة أبرزها الاعتماد على السوق الحرة في عملية تأمين الشبكات وكذلك مسالة الاختيار ما بين الاحتكار وبين الحماية فطبيعة المواجهة الأمنية تتطلب قدرة عالية على التحكم ولكن السعي نحو مكافحة الاحتكار والقطاع الخاص قد أفقدت الولايات المتحدة أو تهددها بالقدرة على السيطرة الأمنية عليها، كما إن قانون الهجرة الذي يمنع شركات تكنولوجيا المعلومات من تعيين كوادر أجنبية أدي ذلك إلى تكلفة عالية مما اثر على عائدات تلك الشركات على قطاع الأمن. كما إن القطاع الخاص والسيطرة على الموظفين الذي يعملون في تلك القطاعات يشكلون عبئا امنيا إضافيا، ولعل تردد الولايات المتحدة في صفقة تولي شركة إماراتية أدارة ستة موانى مبعثه القلق الأمني بما كان قد يتضمن خروجها جزئيا عن ممارسة سيطرتها الأمنية، لذا فان هناك حساسية خاصة تجاه القطاع الخاص في قطاعات معينه وفي ظل أهمية تشجيع الاستثمارات والتزامات اتفاقيات التجارة الدولية

وفي اجتماع وزراء خارجية منظمة المؤتمر الإسلامي في الرابع عشر من شهر مايو ٢٠٠٧ والذي عقد في باكستان طرحت مصر مبادرة لاستصدار قرار إسلامي لمكافحة استخدام الإرهابيين لشبكة الإنترنت، وفي الثلاثين من شهر مايو اتفقت دول الاتحاد الأوروبي بقيادة ألمانيا علي مسودة تفاهم لمراقبة الإرهاب عبر

---

(1) موقع جريدة الجزيرة السعودية، ١٢-٧-٢٠٠٧ (http://www.al-jazirah.com.sa/evillage/30112002/hk.htm)

(2) **Securing Cyberspace for the 44th Presidency**, A Report of theCSIS Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies, US, Washington, DC,December 2008,pp 11-77.

الإنترنت وفي السادس من شهر يونيو ٢٠٠٧ نجحت سلطات الأمن السعودية في الإطاحة بثلاثة من رموز الترويج للأفكار الإرهابية لتنظيم القاعدة[1]، وفي ١٨ ابريل ٢٠٠٨ قرر وزراء العدل في الاتحاد الأوروبي تجريم التحريض على ارتكاب أعمال إرهابية والعمل على توفير الآليات المناسبة التي تسمح للأنظمة القضائية في كافة أنحاء الاتحاد الأوروبي بمقاضاة المجرمين الذين ينشرون دعاية عنيفة تتمثل في عرض معلومات حول تكتيكات إرهابية أو إرشادات حول كيفية صنع عبوات أو متفجرات وفي تحريض الآخرين على ارتكاب أعمال إرهابية، وظهرت محاولات لتوكيل شرطة يوروبول الأوروبية مهمة مراقبة الإنترنت وفتح المركز القومي لحماية البنية التحتية الأمريكي حواراً فعالاً مع المجتمع الدولي شمل مشاركة المركز في المنتدى الثلاثي للتعاون الدولي لتأمين المعلومات في السويد لمجموعة الدول الثمانية-G) (8 ومع مجموعة ليون (المجموعة الفرعية لجرائم التقنية العالمية).

وخلال عام ٢٠٠٧ اجتمع ممثلو المركز القومي مع مسئولين حكوميين، في الولايات المتحدة وفي الخارج، من أستراليا، وكندا، والد نمارك، وفرنسا، وألمانيا، وإسرائيل، واليابان، والنرويج، وسنغافورة، والسويد، والمملكة المتحدة، ودول أخرى للبحث في مسائل حماية البنية التحتية مع نظرائهم ويتصل مركز المراقبة في المركز القومي لحماية البنية التحتية بمراكز المراقبة لعدد من الدول[2].

وتبنت بعض الدول الاوروبيه إجراءات حماية بالتعاون مع الولايات المتحدة فضلا عما تسعى إلية الدولة في إطارها الداخلي من صياغة إطار تشريعي وقانوني يتعامل مع ظاهرة الجرائم المستحدثة والجرائم الالكترونية. وتوجد لدى المجلس الأوروبي الذي يشرف على كثير من المعاهدات القانونية اتفاقية حول الجريمة الالكترونية يعود تاريخها إلى لعام ٢٠٠١ ومن خارج أوروبا وقعت عليها الولايات المتحدة واليابان.

وكما دأبت بعض الدول إلى اختبار دفاعاتها في مقابل هجمات الكمبيوتر كإجراء مناورات داخلية لاختبار قدراتها على الدفاع، بل وهناك مناورات مشتركة، فمثلا شاركت قوات حليفة من بريطانيا وفرنسا وبلجيكا والولايات المتحدة بين ٣- ٥ أكتوبر ٢٠٠٧ مناورات أطلق عليها اسم "وايكومب واربيور" استهدفت إحباط هجوم عنكبوتي على أوربا والعالم الحر، وشاركت في العملية العسكرية نحو ١٥٠ طائرة مقاتلة وهليكوبتر متطورة إضافة إلى قواعد إسناد أرضية وأفاد بيان إن الهدف هو تنسيق الدفاع عن العالم الحر في منطقة معادية تتعرض للإطباق الالكترونية وتمنع الأسلحة المختلفة من الاتصال فيما بينها وتنفيذ مهامها "وتتزعم الولايات المتحدة جهود الدول الغربية في الحرب الالكترونية ومكافحة أي هجمات معادية قد تتعرض لها، والعمل على الحفاظ على تفوقها العسكري وسيطرتها على الفضاء الالكتروني، وتخصص ما يصل إلى ٥٪ من موازنتها العسكرية للإنفاق على تطوير شبكات الأمان الالكترونية في الداخل والخارج.[3]

وقد أقر مجلس الشيوخ الأميركي في ٣ أغسطس ٢٠٠٦ اتفاقية مجلس أوروبا الخاصة بالجرائم الالكترونية "السبريانية"، وهي اتفاقية متعددة الأطراف لمواجهة مشاكل الجرائم المتصلة بالكمبيوتر

---

(1) عادل عبد الصادق "مكافحة الإرهاب عبر الإنترنت :التحديات والفرص "، دراسات سياسية، جريدة الأهرام، ٢٠ مايو ٢٠٠٧ .

(2) بول روجرز ،" حماية أميركا ضد الإرهاب عبر الإنترنت"، موقع وزارة الخارجية الأمريكية ، اخر زيارة (٢٠- ٣- ٢٠٠٦) (http://usinfo.state.gov/journals/itps/1101/ijpa/focus4.htm)

(3) جريدة الحياة اللندنية ٣٠ -١١-٢٠٠٧ ..

ولجمع الأدلة الإلكترونية [1]، و أعلنت ألمانيا إعداد برنامج لتطوير فيروسات وقامت بتطوير فيروسات حاسوب تهدف إلى مراقبة من تصفهم بالإرهابيين، ورصد أي هجمات محتملة والمراقبة الجنائية عن طريق الإنترنت لمن يشتبه فيهم بالإرهاب والذي واجه تحديات انتهاك حقوق الإنسان وذلك بعد إقرار محكمة ألمانية في فبراير ٢٠٠٧ بان التجسس عبر الإنترنت يحتاج إلى منح سلطة قانونية خاصة، و تم عقد مؤتمر في أغسطس ٢٠٠٧ بهدف تجنيد قراصنة الكمبيوتر في الحرب على الإرهاب وذلك بمشاركة مؤسسات أمنية أمريكية حيث شارك ٦ آلاف من القراصنة ومحترفي الكمبيوتر في هذا المؤتمر، وهدفت الولايات المتحدة من هذا المؤتمر لمشاركة جهودها في مكافحة الإرهاب عبر الإنترنت وتبادل المعلومات مع أشخاص من خارج المؤسسات الأمنية وذلك على أمل أن تكسب محترفي الكمبيوتر كحلفاء في مجال الأمن الرقمي. وخاصة مع إدراك أن المرحلة المقبلة من مكافحة الإرهاب والجريمة ستتطلب الاستعانة بأذكى العقول التقنية لخوضها، وأن هذه العقول ستوفر مبالغ ضخمة تضطر الحكومة الأمريكية لدفعها إلى القطاع الخاص.

وتسعى روسيا لصياغة مقترحات لتشديد العقوبات على استخدام الإرهابيين لشبكة الإنترنت ، واتخاذ تدابير صارمة لإيقاف انتشار أفكار الإرهاب والتطرف ، واقترح احد الخبراء الروس إرساء جهاز للأمن على غرار جهاز يوروبول للشرطة الأوروبية مكلفاً بحراسة ومراقبة شبكة الإنترنت بما فيها عمليات التحايل والقرصنة التي تتعرض لها في المستقبل، وقامت المفوضية الأوروبية في بروكسل بتنظيم مؤتمر أوروبي عام حول هذه المسالة في شهر نوفمبر٢٠٠٨ وهو مؤتمر جمع مختلف الأجهزة الأمنية الأوروبية والمتعاملين الرئيسيين في شبكة الإنترنت وبعض الخبراء والمختصين ومراقبين عن الدول الأجنبية.

وتمتلك أوروبا الموحدة حاليا شبكة خاصة تسمى الوكالة الأوروبية لأمن المعلوماتية ENISA (the European Network and Information Security Agency) ومقرها أثينا باليونان ومكلفة بمراقبة القرصنة الالكترونية داخل المجال الأمني الأوروبي.[2] وكانت المملكة المتحدة قد اقترحت قيام منظمة دولية للأمن ( World Security Organization (WSO ، تعنى بمكافحة هجمات الفضاء الإلكتروني وتوفير الأمن للمستخدمين والحكومات وذلك على سياق الجهود الدولية في مواجهه الأخطار التي تأتي من مجالات الجو والبحر والفضاء وتم عقد اجتماع كان محل اهتمام رجال الأعمال والقطاع الخاص وأجهزة الاستخبارات والشركات العاملة في تكنولوجيا المعلومات والأكاديميين والسياسيين ، وذلك بهدف إطلاق مبادرة عالمية اقوي من الانتربول "Interpol". [3]

وجذب حادث تعرض استونيا لهجوم الكتروني في مايو ٢٠٠٧ والحرب الجورجية الروسية في أغسطس ٢٠٠٨ الاهتمام مجددا بأهمية الأمن الالكتروني ، وفي حالة استونيا تم القيام بإجراءات فورية لمواجهه هذا الهجوم، وتم تشكيل فرق طوارئ الكمبيوتر الأستونية وأعقبها اهتمام العديد من الحكومات لتشكيل فرقها الخاصة.[4] وتعد الولايات المتحدة أكثر الدول التي يتم فيها القيام بأنشطة تخريبية باستخدام

---

(1)- مجلس الشيوخ الأميركي يصادق على اتفاقية الجرائم السبرانية
http://usinfo.state.gov/ar/Archive/2006/Aug/10-69758.html

(2) الاتحاد الأوروبي يتصدى للقرصنة الالكترونية ،" وكاله الإنباء السعودية ، ٢٣ مايو ٢٠٠٧

(3) Will Sturgeon," **Cyber-terror plan panned as "barmy"World Security Organisation is a non-starter...**" silicon.com, 9 February 2005

(4) جون رايان،" حرب المعلومات": تهديد جديد، وسلاح ذو حدّين" الأخطار المتصاعدة: التهديدات الأمنية الناشئة والمتزايدة ،مجلة حلف الناتو ،العدد الرابع شتاء ٢٠٠٧ .

الكمبيوتر كما انه في الوقت نفسه يعد أغلب البرامج التخريبية أمريكية الأصل كما الشركات الأمريكية توفر استضافة للمواقع الإرهابية ،وتوجد في الولايات المتحدة عصابات تشكل حلقات معقدة ذات خبرة تقنية عالية ، وهناك منافسة عنيفة في عالم الجرائم التقنية مما يخفض من أسعار البيانات المالية المسروقة .[1] وتأتي الولايات المتحدة أيضاً على رأس قائمة الدول التي تشهد أنشطة شبكات أجهزة " البوت " وهي أجهزة كمبيوتر يتم التحكم بها عن بعد ويتم تشغيلها لتقوم بنشر برامج متطفلة مزعجة غير مرغوب فيها وتجري أعمالاً تخريبية ويحدث ذلك دون علم صاحب الجهاز الأصلي وبروز رسائل غير مرغوب فيها.[2]

وهناك تنسيق بين الشرطة البريطانية ومكتب التحقيقات الفيدرالي الأميركي من أجل إنشاء قاعدة معلومات دولية، هدفها الإيقاع بمن يصنفونهم إرهابيين ومجرمين، وأنشئت دول التحالف ضد الإرهاب (أميركا وبريطانيا وكندا ونيوزيلندا)، مجموعة عمل (كونسورتيوم) للمعلومات الدولية، من اجل التخطيط لإستراتيجياتها في مجال مكافحة الإرهاب والجريمة المنظمة وسيتم بموجب البرنامج المقترح، تبادل صور قزحيات العين وراحة اليد وبصمات أصابع المطلوبين ومعلومات شخصية أخرى، بين أجهزة الأمن في الدول الأربع. ويتوقع أن تحتوي شبكة المعلومات المشتركة في هذا الإطار، بيانات تتعلق بملايين المشبوهين. ويهدف البرنامج إلى تشجيع البحث المتقدم، وتبادل المعلومات على نطاق دولي، ما يؤسس لمنبر تقني لتبادل المعلومات الشخصية عن الإرهابيين والمجرمين المطلوبين.

واهتمت اليابان بسرعة التصدي لخطر الإرهاب الإلكتروني بعد اختراقات عديدة لأنظمة الكومبيوتر الحكومية، واستطاع المخترقون إصابة الموقع الحكومي الياباني ويمحوا بيانات مهمة تتضمن إحصاءات عن عدد السكان، وفي حالة أخرى تمكن المخترقون من نشر رسائل تنتقد الموقف الياباني الرسمي من مذابح نانكين التي يتهم بارتكابها الجنود اليابانيون في الصين عام ١٩٣٧ على موقع وكالة (وزارة) التنسيق والإدارة ووكالة (وزارة) العلوم والتكنولوجيا، وفي ألمانيا هناك اهتمام بتمتع البلاد بحماية جيدة ضد الاعتداءات عن طريق الإنترنت بشكل عام، وتأمين أنظمة الكومبيوتر الحكومية بشكل كبير منذ الاعتداءات الإرهابية على أمريكا، وقد ركز المكتب الاتحادي للأمن وتكنولوجيا المعلومات الذي أسسته ألمانيا بشكل خاص على كل ما يتعلق بتأمين البنية التحتية لتكنولوجيا المعلومات. وقد خصصت وزارة الأمن الداخلي الأمريكي ١٢، ٥ مليون دولار عام ٢٠٠٤ للأمن الرقمي وفي عام ٢٠٠٥ وصلت لـ ١٧، ٥ مليون دولار و١٥ مليون دولار عام ٢٠٠٦ و٢٠٠٧ وهذا يعكس خطة أمنية إستراتيجية ضد الإرهاب الإلكتروني.

ودعت مجموعه الثماني الصناعية في ١١ مايو ٢٠٠٤ بالعمل على تطوير القوانين المحلية من اجل بناء قدرات عالية لمواجهه الاستخدام الإجرامي والإرهابي للانترنت وان تسعى الدول لتحسين قوانينها التي تجرم الاستخدام السيئ للكمبيوتر والإنترنت وما يساعد ذلك في تسريع حركة التعاون حول القضايا المتعلقة بالتحقيقات[3] . وأعقب ذلك دخول الاتفاقية الأوربية لمكافحة الجريمة الالكترونية حيز التنفيذ في ايوليو ٢٠٠٤، والتي مثلت إضافة هامة في سبيل تحقيق المواءمة القانونية والتعاون الدولي في مواجهه الجريمة

---

(1) **The National Strategy to Secure Cyberspace.** Washington, whitehouse, February 2003. p 61 . Also available online at: (http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf)

(3) G8 Justice and Home Affairs Communiqué, Washington DC, May 11, 2004, p.10.

الالكترونية، كما اتخذت نفس خطوات الاهتمام لدى منظمة التعاون الاقتصادي لأسيا والمحيط الهادي، وأعلنت منظمة الدول الأمريكية في ٣٠ ابريل ٢٠٠٤ قرارا بتبني الاتفاقية الأوربية لمكافحة الجريمة الالكترونية ومبادئها ودعم الجهود الدولية في هذا الصدد من أجل التوصل إلى إطار قانوني دولي لمكافحة الجريمة الالكترونية، وأخذت الجهود الإقليمية في الاهتمام على مستوى المنظمات كمنظمة المؤتمر الإسلامي التي تبنت الدعوة إلى تجريم استخدام الإنترنت في العمل الإرهابي في قمتها بباكستان عام ٢٠٠٧ وكذلك على مستوى جامعه الدول العربية وخاصة على مستوى اجتماعات وزاري الداخلية العرب.

## المطلب الثاني:
## المبادرات الدولية لتعزيز امن الفضاء الالكتروني

كان هناك العديد من المبادرات التي تم اتخاذها لمواجهة ظاهرة الاستخدام غير السلمي للفضاء الالكتروني وتنوعت تلك المبادرات من جانب الحكومات والقطاع الخاص والمجتمع المدني والمنظمات الدولية والتي من أهمها او من ضمنها :

أولا: مبادرة الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب الإلكتروني IMPACT

استلزم الطابع الدولي للإرهاب الالكتروني طابعا دوليا حيث لا يمكن أن تقوم دول بمفردها في جهود المكافحة، وفي بادرة هي الأولي من نوعها في العلاقات الدولية أعلنت ماليزيا إطلاق مبادرة في مايو ٢٠٠٦ تحت مسمى " الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب الإلكتروني IMPACT" وذلك على هامش انعقاد المؤتمر الدولي الخامس عشر حول تكنولوجيا المعلومات، وتهدف هذه المبادرة لحشد الجهود الدولية من جانب القطاعات الحكومية والقطاع الخاص والمجتمع المدني لمواجهه تزايد الأخطار التي يمثلها الإرهاب الإلكتروني، كما هدفت هذه المبادرة إلى جمع الرؤى والأفكار حول التدريب وتبادل الخبرات، وتعمل كمنظمة دولية غير هادفة للربح وتهدف إلى جمع الحكومات والقطاع الخاص والأكاديميين وقادة صناع تكنولوجيا الاتصال وخبراء امن المعلومات لدعم قدرة المجتمع الدولي في عملية المنع والوقاية من الأخطار الالكترونية وتكونت تلك المبادرة من إنشاء أربعة مراكز هي مركز تنمية المهارات والتدريب ومركز لشهادات الأمن والبحث والتنمية ومركز دعم التعاون الدولي ومركز الاستجابة و الطوارئ الدولية [1] .

وجذبت تلك المبادرة العديد من الشركاء الدوليين وضمت ما يزيد على ٣٠ عضوا من أعضاء الاتحاد الدولي للاتصالات، من اجل تحسين قدرات العالم على مواجهة خطر الإرهاب عبر الإنترنت وتم عقد القمة الأولى للأمن الاليكتروني في العاصمة الماليزية كوالالمبور في ٢٣ مايو ٢٠٠٨ وضمت خبراء من كافة دول العالم لبحث كيفية مواجهة الإرهاب الإلكتروني. وتقوم مؤسسة "إمباكت "بالعمل على مساعده أعضائها بالتدريب وبتنمية قدراتهم، كما ستعمل على دعم القوانين وتطبيقها بشأن الإرهاب الإلكتروني. وقد ساهمت ماليزيا ماديا في إنشاء إمباكت، وبقى دور الولايات المتحدة وأوربا ودول الشرق الأوسط في تقديم

---

(1) New Global Partnership to Fight Cyber Terrorism Seeks the Business., Zeichner Risk Assessment Newsletters , " Vol. 1, No. 30 - May 30, 2008.

المساعدة للمنظمة، إذ أن كل دول العالم المتحضر تشترك فيما بينها في الاهتمام بضرورة مواجهة أخطار الإرهاب الإلكتروني وحماية أمن وسلامة العالم القائم على تقنية المعلومات .

ثالثا : إنشاء مواقع على الإنترنت للمكافحة والرصد ومراكز الأبحاث والرصد والتحليل:

تم إنشاء العديد من مواقع الإنترنت لمكافحة الإرهاب الإلكتروني والأمن الرقمي حيث أصبحت بمثابة مؤسسات فكرية وفنية لدعم الأمن الرقمي وكانت تلك المواقع أما بمبادرة حكومية أو من جانب القطاع الخاص أو من جانب المجتمع المدني. بالإضافة إلى مواقع الشركات العاملة في تكنولوجيا الاتصال والمعلومات. وتتضمن تلك المواقع أقساماً خاصة لمكافحة القرصنة والجريمة الالكترونية والإرهاب عبر الإنترنت كما تتضمن إطلاق العديد من المبادرات لحماية نظم المعلومات وبرامج الحماية الحديثة.

كما تمثل نقطة التقاء لخبراء امن المعلومات والسياسيين ورجال الأعمال والحكومات للتباحث حول ماهية خطر الإرهاب الإلكتروني وكيفية مواجهته. مثل :مجموعه "SITE"للاستخبارات وهو يعد كجهاز استخبارات متخصص في رصد الإرهاب عبر الإنترنت ومراقبته ودراسة المصادر الأولية للإرهابيين والمرجعيات الفكرية لهم وترجمة أحاديثهم، ومراقبة دعاية الإرهابيين، وتقدم تلك المجموعة خدماتها للشركات والحكومات والمؤسسات الأكاديمية والمنظمات غير الحكومية و وسائل الإعلام والصحفيين، كما تقوم بفك شفرات المواقع الإرهابية والحصول على المعلومات وتراقب المشتبه فيهم بالإرهاب، [1]

رابعا : تعزيز الاتفاقيات الدولية: .

أكدت كافة التفاعليات الدولية على أهمية تفعيل الاتفاقية الأوربية لمكافحة الجريمة الالكترونية باعتبارها تشكل الأساس الدولي للنظر في القوانين الوطنية بما يتلاءم مع طرق مواجهتها، وخاصة انه لا توجد دولة واحدة لديها القدرة على السيطرة الكاملة على الفضاء الالكتروني ،حيث إنها مورد عالمي — كالبحار تماماً. وقد دفعت سياسة حماية البحار والمحيطات في الماضي، إلى تطوير معايير دوليّة جديدة للسلوك، مثل القوانين العرفية الشكلية الرامية لحماية الوصول إلى البحر. وقد أخذت إجراءات حماية نظم المعلومات ضد هجمات الفضاء الإلكتروني المزيد من الاهتمام مع زيادة معدلات النمو في الهجمات وفي طبيعة الخطر وأخذت تلك الإجراءات تركز على استخدام التكنولوجيا لمراقبة شبكات الكمبيوتر والمستخدمين.

وفرض ذلك إشكاليات خاصة بالموازنة بين حماية المواطنين المنشآت من التعرض للخطر من التعرض للخطر وفي نفس الوقت العمل على الحفاظ على حرياتهم والحق في التعبير والخصوصية وهذه الحريات مدعمه وفق القانون الدولي وتمت حمايتها في العديد من القوانين الوطنية والعديد من المؤسسات في العديد من الدول، ولذا فقد كان النظام الدولي بحاجة إلى مواجهه الجريمة الالكترونية والإرهاب مع الحفاظ على القيود التي تفرضها المبادئ كما حددتها الأطر القانونية للدول الأطراف.

وعلى نحو يعمل على الحفاظ على الحريات المدنية وتقوية القانون للحفاظ على النظام والأمن العام، وأصبح هناك نوعان من فرض الحماية في الفضاء الإلكتروني: الأول وقائي aprotective والثاني يتعلق برد الفعل reactive ويعمل كلا البعدين في سبيل دعم تامين الفضاء الإلكتروني، حيث يهدف البعد الحنائي

[1] يمكن زيارة موقع مؤسسة "سايت " على الانترنت على الرابط التالي ( http://www.siteintelgroup.org)

لمواجهه المجرمين من خلال اتخاذ الإجراءات التي تهدف إلى إنكار الخدمة أو جعل الهدف المحتمل اقل قابلية للهجوم، ويركز هذا البعد على الدفاع ويتضمن تصميم المزيد من أمن بروتوكولات الإنترنت واستخدام حوائط النار وغيرها من الإجراءات الأمنية كاحتواء الخطر من خلال التحقيقات الفعالة والرصد والعقاب، وكلا البعدين يتضمن المراقبة والقيام بنشاط غير تقليدي ويعتمد البعد الحنائي على تصورات خبراء امن الكمبيوتر، بينما توجد عدد من العقبات أمام الأمن الالكتروني مثل قيود الميزانية والتعقيد الفني وعدم وضوح المسئوليات وضعف معايير الأمن في المنتجات، ونقص الوعي، ونقص أدوات الأمن الملائمة وامن المعلومات الشخصية والخصوصية والقضايا الأخلاقية ."[1]

خامسا : المناورات والتدريب

في محاولة لاختبار جاهزية النظم الالكترونية لمواجهه هذا الخطر قامت الولايات المتحدة بعقد " مناورة الكترونية " في فبراير ٢٠٠٦[2] لمده أسبوع كامل، و سميت بعاصفة الحواسب ('Cyber Storm 1) ، حيث قامت بها أجهزه الاستخبارات الأمريكية حيث وضعت البني التحتية الحيوية الأمريكية التي تشمل شبكات الكهرباء والنظم المصرفية تحت محاكاة لهجوم على مدار أسبوع كامل تحت رعاية وزاره الأمن الداخلي واشترك في لعبه الحرب هذه ١١٥ وكاله تراوحت من وكاله الاستخبارات المركزية ومكتب التحقيقات الفيدرالي إلى الصليب الأحمر الدولي .

وتتعلق أهداف "cyber storm" بأنها صممت لاختبار الاتصالات والسياسيات والإجراءات في حالة التعرض لهجمات الفضاء الإلكتروني المتنوعة والقدرة على تحديد مراكز الخلل وتحسين الإجراءات المطلوبة، وضمت الأنشطة عملية التنسيق بين خدمات الطوارئ وما بين القطاعات الحكومية وغير الحكومية ومتطلبات دعم الأمن الالكتروني، والعمل على تحديد ميكانيزم لتبادل المعلومات العامة والخاصة، والعمل على تحييد البنية التحتية الطبيعية والالكترونية، والعمل على رفع الوعي بخطورة هجمات الفضاء الإلكتروني على الأمن والاقتصاد القومي

وتم إجراء مناورة أخرى في فبراير ٢٠٠٨ سميت بـ " عاصفة الحواسب (Cyber Storm II) ، حيث شارك فيها بالإضافة إلى الولايات المتحدة استراليا وكندا ونيوزيلاندا والمملكة المتحدة بالإضافة إلى وزارة الدفاع والعدل الأمريكية و تمت دعوة تسع ولايات أمريكية للمشاركة هي كاليفورنيا وكلورادوا وديلاور والينوى وميتشجان ونورث كارولينا وبنسلفانيا وتكساس وفيرجينيا ، هذا بالإضافة إلى ٤٠ شركة من القطاع الخاص . وأخذت مناورة عاصفة الحواسب ٢ زهاء ١٨ شهرا في الإعداد وتكلفت ٦، ٢ مليون دولار.

خامسا : دور المنظمات الإقليمية :

أصبح هناك العديد من المنظمات التي تم إنشاؤها بمبادرة من الحكومات أو من القطاع الخاص وبالتعاون فيما بينهما أو بدعم من الاتحاد الدولي للاتصالات أو الأمم المتحدة، و منظمة الأمن و التعاون الاقتصادي والتي كانت أكثر فاعلية في مجال الأمن الالكتروني وخاصة ما يتعلق بالموازنة ما بين الحفاظ

---

(1) Seymour E. Goodman & Abraham D. Sofaer (eds) ," **The Transnational Dimension of Cyber Crime And Terrorism** ", Ekaterina A. Drozdova," Civil Liberties and Security in Cyberspace" Ch.5 , the Board of Trustees of the Leland Stanford Junior University,2001,pp. 183 – 222

(2) Cyber Storm Exercise Report ," **Department of Homeland Security National Cyber Security Division**", DHS, September 12, 2006

للإطلاع على تقرير وزارة الأمن الداخلي الأمريكي(www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf)

على الأمن وحماية الخصوصية وعملت على تطوير مجموعه من الوسائل لمكافحة الإرهاب الإلكتروني وفيروسات الكمبيوتر والقرصنة والأخطار التي ترتبط بها .[1]

وهناك المركز الدولي للأمن والتعاونCISAC والتحالف الدولي للخدمات والتكنولوجيا WITSA والوكالة الدولية لأمن المعلومات والشبكات والتي أسسها الاتحاد الأوربي لتحقيق مستوى عالمي من امن المعلومات والشبكات داخل الاتحاد الأوربي والعمل على نشر الوعي بالأمن الالكتروني لخدمة المستهلكين والمواطنين وقطاع الأعمال والقطاع الخاص داخل الاتحاد الأوربي، كما إن هناك العديد من المبادرات والمنظمات التي أقامها القطاع الخاص والشركات العاملة في مجال تكنولوجيا الاتصال والمعلومات، وهناك العديد منها مثل Computer Security and Incident Response Team (CSIRT)..

وأنشئت في العديد من الدول للحماية من خطر التعرض لأخطار أنظمة المعلومات وتقديم الخدمات الأمنية في كافة القطاعات الأكاديمية والتجارية وحماية البنية التحتية والقطاع الحكومي والعسكري والوطني والمشروعات الصغيرة والمتوسطة، وهناك منتدى فرق الأمن والاستجابة (FIRST forum of incincident response and security team، وهي منظمة عالمية لمواجهه الحوادث التي تتعلق بأمن المعلومات وتبادلها والعمل على بناء بيئة الكترونية أمنة. وقامت العديد من الدول بإنشاء تلك الهيئات داخلها وقد أتم مجلس أوربا COE منذ أواخر الثمانينات العمل على دعم التعاون العالمي ضد المخاطر التي تفرضها جرائم الكمبيوتر والمرتبطة بالإنترنت.

وفي عام ١٩٨٩ أصدر مجلس أوربا دراسة وتوصيات تتعلق بالحاجة إلى قوانين جديدة تتعامل مع الجرائم التي ترتكب من خلال هذه الشبكات، وصدرت دراسة أخرى عام ١٩٩٥ عن إرساء المبادئ التي تتعلق بالتعامل مع تلك الظاهرة قانونا، وجاء اتفاق مجلس أوربا في عام ٢٠٠١ حول الجريمة الالكترونية ليمثل حجر الزاوية في مكافحة تلك الجرائم عالميا. واهتمت منظمة ابيك APEC وهي منظمة التعاون لدول أسيا والمحيط الهادي و اهتمت دولة بالخطر العالمي الذي يمثله الإرهاب وأهمية زيادة معدلات الحماية للبنية التحتية المعلوماتية والعمل على إيجاد إطار شامل يضع قوانين للأمن الالكتروني وما يتواكب مع المعايير الدولية وخاصة الاتفاقية الأوربية لمكافحة الجريمة الالكترونية. وعملت المنظمة على تشكيل مجموعه عمل للاتصالات والبنية التحتية من اجل العمل على زيادة قدرة الأعضاء على الاهتمام بالخطر وتحقيق التعاون الأكبر ما بين الحكومات والقطاعين العام والخاص، وكذلك العمل على تطوير وتنفيذ سياسات خاصة بالاتصالات والمعلومات ودعم الموارد البشرية وعقدت مجموعه العمل الخاصة بالمنظمة ثلاثة مؤتمرات في بانكوك وهانوي وسيول أعوام ٢٠٠٣و٢٠٠٤و٢٠٠٥ .

سادسا : موقف حلف شمال الأطلنطي من هجمات الفضاء الإلكتروني:

جاء اهتمام حلف الناتو باعتباره المظلة الأمنية لأوربا في شكل خطوت عملية تمثلت في نص الدليل السياسي الشامل لحلف الناتو الذي تبناه رؤساء دول وحكومات الحلف في نوفمبر ٢٠٠٦، على تعزيز "القدرة على حماية أنظمة المعلومات ذات الأهمية الكبيرة بالنسبة للحلف، ضد الهجمات على الإنترنت"،

---

[1] Myriam Dunn," Towards an International Regime for the Protection of Cyberspace?", CIIP Research Group, Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology), Switzerland, Volume 2, Number 11 , May 2004 ,pp10-11

كما إن الهجوم على استونيا أثار قدرة الحلف على الدفاع ضد تلك الهجمات وامكانية تطبيق المادة (٥) من اتفاقية الحلف التي تقر بان إي اعتداء على احد أعضاء الحلف يمثل اعتداء على باقي دوله ". وعلى الرغم من أن حلف الناتو اعتبر أن الهجوم الالكتروني لا يكون كعمل عسكري إلا إذا تم تحديد مسئولية مرتكبيه قام الحلف بتبني سياسة دفاعية في الفضاء الإلكتروني فيما عرف بـ" a new policy on cyber defence "[1] وذلك إلى جانب امن الطاقة في قمة بوخارست والتي عقدت في ٤ ابريل ٢٠٠٨، وهي القمة التي شهدت مشاركة روسيا لأول مرة منذ تأسيس الحلف عام ١٩٩٢ في إطار التعاون بين روسيا وحلف الناتو [2] .

وقد وصف "Suleyman Anil" رئيس وحدة الدفاع الالكتروني التابع لحلف الناتو بان الإرهاب الإلكتروني يفرض خطورة على الأمن القومي لاتقل عن خطورة هجمات الأسلحة الصاروخية، وخاصة إن هجمات الفضاء الإلكتروني التي تستهدف البنية التحتية لا يمكن عمليا إيقافها، ومن ثم فان الدول بحاجة إلى تقوية نظمها المعلوماتية ومع ما يمثله الإرهاب الإلكتروني من مشكلة عالمية مستقبلية، وقام الحلف بإنشاء وحدة عمل في قمة بوخارست في ابريل ٢٠٠٨ خاصة بدراسة احتمال تعرض أعضاؤه لهجمات مماثلة لما تعرضت له استونيا[3] .

وتم تشكيل قيادة دفاع وفرق خاصة عبر الفضاء الإلكتروني The Cyber Defence Management Authority (CDMA) للتصدي لأي محاولة لشن هجمات الكترونية عبر الإنترنت، وذلك للتنسيق فيما بين دول الحلف في حال تعرض احدهما لهجمات الفضاء الإلكتروني والتعاون الأمني في حماية بنياتها الأساسية، و مثل ذلك تحولا في سياسة الحلف الأمنية للتركيز على حماية أنظمته الداخلية عن طريق استخدام وحدة Nato ComputerIncident Response Capability (NRIC). لحماية الدول الأعضاء من هجمات الكمبيوتر. كما يسعى الحلف إلى إنشاء مركز امتياز في الدفاع الالكتروني في "تالين" عاصمة استونيا سيفتتح رسميا في عام ٢٠٠٩ [4].

وفي مايو عام ٢٠٠٨ وقعت ٧ دول من أعضاء حلف الناتو على وثيقة تقضي بإنشاء دفاع مشترك الكتروني CCO، وإنشاء مركز للخبرة والتدريب COE في عاصمة استونيا ويهدف مركز الخبرة إلى البحث والتدريب والتطوير المشترك حول حرب الفضاء الإلكتروني بالتعاون مع ألمانيا وايطاليا ولاتفيا وليتوانيا وسلوفاكيا وأسبانيا واستونيا، كما يأتي اتفاق الدفاع المشترك بشان الهجمات الالكتروني بعد عام من تعرض استونيا إلى هجمات الكترونية كبيرة، كما قام الحلف بدعوة وزراء دفاعه بتطوير سياسات دفاعية خاصة بشان الهجمات الالكترونية في اكتوبر٢٠٠٧.

---

[1] وذلك إلى جانب تبني الحلف خلال الاجتماعات قضايا الاتفاق حول تطوير القدرات الدفاعية والحد من التسلح، ومنع الانتشار النووي، واهمية قوة الرد العسكرية التابعه للحلف، ودعم التعاون الأمني وامن الطاقة. للمزيد انظر ايضا مجلس التعاون و روسيا وحلف الناتو، للمزيد يمكن الإطلاع على الرابط التالي :أخر زيارة (١٢- ٧- ٢٠٠٨ ).

(http://www.nato-russia-council.info/htm/EN/news_41.shtml )

[2] البيان الختامي للقمة انظر الرابط التالي (أخر زيارة ٢٠- ٤- ٢٠٠٧).

(http://www.nato.int/docu/update/2008/04-april/e0403f.html)

[3] Nick Heath," **Nato: Cyber terrorism 'as dangerous as missile attack'**" silicon.com, 7 March 2008, http://software.silicon.com/security/0,39024655,39170300,00.htm

[4] Nick Heath," **Nato allies form cyber defence command,** silicon.com, 8 April 2008

وقد عرض اقتراح على دول الحلف لتشكيل مديرية أمن موحدة لحلف الناتو للتعامل مع الإرهاب، والتحديات الأمنية التي يرون أن مصدرها الصين وإيران.، ويمتد التعاون الأمني إلى بصمات أصابع المطلوبين عبر ضفتي الأطلسي، إلى وضع استراتيجيات مشتركة لمكافحة الإرهاب. وأطلق على البرنامج المقترح اسم "خادم في السماء"وتم التأكيد على إنه لا يمكن لحلف الأطلسي والاتحاد الأوروبي ولا أي دولة التعامل مع التهديدات الأمنية الجديدة بمفردها، فيما سيستغرق تطوير مؤسسات أمنية جديدة وقتاً طويلاً.[1] وتم تبني تلك الدعوة عمليا في أوائل عام ٢٠٠٨ بإنشاء سلطة إدارة الدفاع الالكتروني التي يكون من مهامها إدارة عملية الدفاع في مواجهه تلك الهجمات من خلال الاتصالات ونظم المعلومات التابعة للحلف والعمل على دعم حلفاء الحلف في مواجهه تلك التهديدات التي تشكلها تلك الهجمات[2].

ويدفع حلف الناتو إلى وجود تبادل المعلومات على مستوى دوله ومن اجل وجود آلية للإنذار المبكّر حول أي نشاط مريب، والكشف عن أي هجوم معلوماتي محتمل. وبدأت بعض الدول الأعضاء في الحلف باتخاذ إجراءات لحماية نفسها من تهديدات عصر الإنترنت بإنشاء فرق وطنية لطوارئ الكمبيوتروجاءت جهود حلف الناتو بالتعاون مع الاتحاد الأوروبي في سبيل الحد من تأثير هجمات الحرب المعلوماتية في المدى القريب. إلى الدرجة التي إذا تم اكتشاف هجوم على موقع تشيكي على الإنترنت بواسطة مستخدم من شبكة فرنسية، على سبيل المثال، فإنه يمكن لفرق طوارئ الكمبيوتر التشيكية أن تطلب من نظيرتها الفرنسية قطع قنوات الاتصال المستخدمة في الهجمات. وهذا ما دفع حلف الناتو لتشكيل فرق خاصة مكلفة بالتصدي لأي محاولة لشن هجمات الكترونية عبر الإنترنت.

وجاء ذلك بعد حادثة من هذا النوع استهدفت المواقع الحكومية في استونيا العضو في حلف الناتو عام ٢٠٠٧ وتلقت استونيا دعما من الولايات المتحدة وألمانيا ورومانيا وايطاليا واسبانيا. وبغية "التعامل مع عواقب" الهجمات الالكترونية شكل الحلف فرقا جاهزة للتدخل في غضون ٢٤ ساعة في الدول المستهدفة كتلك التي سبق إن أنشأها الحلف للرد على هجمات كيميائية، بيولوجية أو إشعاعية محتملة.[3] فمثلا ترى روسيا أن الهجوم ضد نظم اتصالاتها وصناعات القوة الالكترونية لها بما يؤدي إلى اثار كارثية يدخل تماما ضمن استخدام أسلحة الدمار الشامل ، وفي إطار التداعيات الخاصة بالهجوم الالكتروني على استونيا دعا بعض المسئولين الروس إلى إن روسيا تحتفظ بحق الرد في حالة تعرضها لحرب المعلومات باستخدام الأسلحة النووية .

---

(1). وجاء ذلك في تقرير لمؤسسة بحوث صندوق "مارشال" الألماني: وتم اقتراح كخطوة أولى بانجاز اتفاق عبر ضفتي الأطلسي,و إقامة مديرية توجيه للولايات المتحدة والاتحاد الأوروبي وحلف شمل الأطلسي، على أعلى مستوى سياسي».، وكان واضعو التقرير الخمسة، هم: رئيس اللجنة العسكرية السابق لحلف شمل الأطلسي كلاوس نيومان، ورئيس قيادة الأركان البريطاني السابق بيتر انجي، والرئيس السابق لقيادة الأركان المشتركة الأميركية جون شاليكاشفيلي، والرئيس السابق لقيادة الأركان الفرنسية جك لانكساد، والرئيس السابق لقيادة الأركان الهولندية هينك فان دين بريمين ، للمزيد انظر ، جريدة الحياة اللندنية ، ١٦ يناير ٢٠٠٨.

(2) Greg Jaffe, **"Gates Urges NATO Ministers to Defend Against Cyber Attacks,"** Wall Street Journal, June 15, 2007.

(3) James Mulvenon ," Toward a Cyberconflict Studies Research Agenda",in "On the Horizon",O.sami Saydijari,(editor), IEEE computer security ,july/august 2005 , pp64-67 (http://www.cyberconflict.org/pdf/IEEEarticlefinal.pdf)

## المبحث الثالث:
## نحو ميثاق دولي وثقافة عالمية لحماية الفضاء الإلكتروني

**يأتي إلى جانب أهمية إيجاد إطار قانوني يعمل على تنظم ظاهرة الفضاء الالكتروني ويحكم استخداماته السلمية وغير السلمية أهمية وجود ثقافة عالمية للأمن الالكتروني والعمل على نشرها ورفع الوعي العالمي ، ويتناول الباحث ذلك في ثلاثة مطالب الأول يتناول الأمن الالكتروني ضمن إستراتيجية الأمن الدولي ، وأما المطلب الثاني: الفضاء الالكتروني وخصائص المرفق الدولي والتراث المشترك للإنسانية، وفي المطلب الثالث: نحو اتفاقية دولية للفضاء الالكتروني وتعزيز أطر القانون الدولي الحالي .**

### المطلب الأول:
### الأمن الإلكتروني يدخل ضمن إستراتجية الأمن الدولي

انه في عالم متشابك لا يوجد فيه مكان منعزل أصبح أي طرف متصلاً بشبكة تكنولوجيا الاتصال والمعلومات يمكن أن يتأثر إما بالأطراف الأخرى المتصلة على نفس الشبكة أو بطبيعة الأخطار التي تعترض هذه الشبكة وتهدد طبيعة عملها، بما يكون له من انعكاسات اقتصادية وأمنية بما يؤثر على الاستقرار السياسي والاجتماعي، وليعكس ذلك الأيمان القوي بان الثقة والأمن هما محوران مهمان لمجتمع المعلومات العالمي، و أصبحت مسألة الدعم الفني والتشريعي وتوفير جو مناسب لانتشار واستقرار البيئة التكنولوجية من أهم مرتكزاته، وأصبحت الثقافة العالمية الخاصة بالأمن الالكتروني بحاجة للمزيد من الدعم والحصول على المساندة من كافة الأطراف الدولية، وتم التأكيد على ذلك في القمة العالمية لمجتمع المعلومات عام ٢٠٠٣وعام ٢٠٠٥، وتم دعمهما بقرارين لاحقين من الأمم المتحدة.[1]

ويعد الأمنsecurity مفهوماً واسعاً يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم العسكري أو الإرهابي، وتعني كلمة الأمن في مجال الفضاء الإلكتروني إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات، ومن جهة أخرى فان الأمن القومي يعني بحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، وتشير كلمة الأمن إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات.

وظهر مفهوم أمن المعلومات في أواخر السبعينيات حيث كان معروفاً باسم أمن الاتصالات (Communication Security) (COMSEC) وحددته توصيات لجنة أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بأنه يعني "المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بها عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات". وتضمنت النشاطات المحددة لأمن الاتصالات COMSEC أربعة أجزاء هي: أمن التشفير Crypto security، وأمن النقل Transmission Security، و أمن الإشعاع Emission Security والأمن الفيزيائي Physical Security. و يتميز الأمن الإلكتروني بعدد من الخصائص أهمها السرية من خلال التأكيد بأن المعلومات لم تصل لأشخاص

---

[1] **Creation of a global culture of cybersecurity,"** Resolution adopted by the General Assembly", United Nations, Fifty-seventh session , Agenda item 84 (*c*), A/RES/57/23, 31 January 2003. (http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf)

غير مخولة بالحصول عليها والتحقق من هويتها ،والتأكد من صلاحية الاتصال، والرسالة أو مصدرهذه المعلومات.ويتميز الامن الالكتروني بتوافر التكامل الذي يعني جودة أي نظام للمعلومات ومدى صحة ووثوقية نظام التشغيل، وأيضا التكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى تناغم بني المعلومات مع البيانات المخزنة.

وهناك خاصية التوافر والإتاحة من خلال الوصول الموثوق للبيانات وخدمات المعلومات عند الحاجة إليها من قبل الأشخاص المخولين بذلك. وخاصية مكافحة الإنكار من خلال التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانات إلى المرسل إليه، وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع احتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات. وتتضمن عمليات الأمن الالكتروني عدداً من الإجراءات من قبيل مجموعه الأنشطة والإجراءات التكنولوجية وغير التكنولوجية بهدف حماية شبكات المعلومات والاتصال وما تتضمنه من برمجيات ومعدات وأجهزة،وتطبيق إجراءات وأنشطة حمائيه تخدم عمليات التأمين من قبيل البحث والتدريب والتطوير ورفع الوعي، ويعد الأمن الالكتروني أكبر من مجرد أمن المعلومات أو أمن البيانات، وذلك على الرغم من ارتباطهما به وذلك لأن أمن المعلومات يشير إلى كل أنواع الحماية للمعلومات من خلال الحفاظ على الثقة والتكامل والإتاحة والسرية ومكافحة الإنكار.

ويؤثر الاستخدام غير السلمي للفضاء الالكتروني على تهديد الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية للمعلومات، وأصبح هناك مصلحة دولية في الحفاظ على أمن الفضاء الإلكتروني ومن مصلحة كل دولة كذلك على اعتبار أنها جزء من الأمن الجماعي والذي يمكن أن يعمل على ضمان الثقة والأمن والرقابة على شبكات المعلومات والاتصال، ومن هذا المنطلق كان هناك عدد من الآليات للتعامل مع هذه الأخطار.

ومن ثم يصبح تحقيق مكاسب لطرف لا يعني حدوث خسائر لطرف أخر، كما إن حدوث تقدم في مجال المكافحة ولو كان جزئيا فإنه يصب مباشرة في مصلحة جميع الدول، حيث إن هناك حالة من الاعتماد المتبادل بين جميع الدول حول استخدام بنية تحتية واحدة تنتشر في جميع دول العالم، وترتبط ببعضها البعض وتمثل مصالح إستراتيجية للمجتمع الدولي، وهذا ما يشكل أرضية هامة لجعل البنية التحتية الكونية للمعلومات أكثر أمنا واستقلالاً، ويمكن للأطر القانونية الدولية وآلياتها مثل" الانتربول" أن تستخدم في عملية تبادل المعلومات والتحقيقات.

وتعد مكافحة الاستخدام غير السلمي للفضاء الالكتروني معركة غير صفرية حيث أن أي مكسب لطرف أو خسارته يكون متوازنا مع خسائر أو مكاسب الطرف الأخر، وأنه عندما يكون هناك خسائر أو مكاسب لكل الأطراف تكون نتيجة القيمة صفراً، ولذا فإن الهجمات ضد البنية التحتية الكونية للمعلومات لطرف يمكن أن تؤدي بالتبعية إلى أضرار للأطراف الأخرى، وتستخدم تلك الهجمات كأداة إستراتيجية يمكن أن تؤدي إلى التأثير على الإتاحة والثقة والأمان والتكامل لأنظمة المعلومات، والتي يمكن أن تعد على المستوى النظري عملاً من أعمال الحرب ويمكن أن تدخل ضمن اتفاقيات الحد من التسلح أو قانون النزاعات المسلحة الدولية، ومن ثم فإن وجود الآليات والوسائل كقانون النزاع المسلح يمكن أن يتم تطبيقه على تلك الأنواع الجديدة من الأسلحة التي يمكن أن تستخدمها الدول أو الجماعات

الإرهابية، وتواجه مسألة الأمن وتطبيقه في عصر المعلومات بإمكانية استخدام الفضاء الإلكتروني استخداما عسكرياً وتطوير أدوات حرب المعلومات في مقابل الاستخدام المدني الذي يرتبط بالبنية التحتية للمعلومات وصعوبة الفصل بينهما.

وعلى الرغم من وجود ما يزيد على ٢٨ تعريفاً مختلفاً للفضاء الالكتروني إلا أنها تجمع بأن الفضاء الإلكتروني يتضمن فقط مكونات تكنولوجية كالكمبيوتر وشبكات الاتصالات وما يرتبط بها ولكن الفضاء الالكتروني يتضمن أيضا العناصر الخاصة بالمعلومات والعنصر البشري، وهذا لا يعني أن الإنترنت لا يساوي أو يعبر عن الفضاء الإلكتروني ولكن الإنترنت هو جزء من الفضاء الإلكتروني، ولذلك فانه عند الحديث عن الأمن الالكتروني، فانه يجب أن يتم الاهتمام بالعنصر البشري، وأصبحت قضية امن الفضاء الإلكتروني قضية دولية تتطلب إستراتجية مرنه تتواءم مع المتغيرات المستمرة سواء في الآليات أو في التكتيكات الخاصة بالأمن مقابل التطور المستمر في الأخطار، ويرجع ذلك إلى الطبيعة المتغيرة للفضاء الالكتروني وفقا للعامل الإنساني الذي يتعامل معه وكان لظهور الفضاء الالكتروني والذي أخذ في التطور والانتشار الهائل تأثير واضح على شئون الأمن الدولي في حالة استخدامه، وحدث تداخل بين البعد الأمني مع الجنائي مع الطبيعة الدولية للفضاء الالكتروني. وعلى الرغم من طابعه الافتراضي بالمقارنة بالطبيعة المادية إلا أنه يعبر عن وجود مادي بشكل خاص، و خصائص مختلفة عن الطبيعة الفيزيائية، ويكون الفاعلون به غير مقيدين بالموقع الطبيعي أو الجغرافي أو الحدود السياسية للدول.

وتصبح الأهداف والعناصر غير قابلة للخضوع والسيطرة من الدول وفق معطيات الفضاء الإلكتروني، وارتبطت القوة العسكرية بالتحكم في أربعه مجالات تتشكل من القدرة على السيطرة على البر والبحر والجو والفضاء الخارجي، وكان الفكر الأمني مرتبطاً بمسالة الدفاع والهجوم عن طريق الجيوش التقليدية أو دعم الحلفاء وكان يتحقق ذلك الأمن عن طريق عده عناصر سياسية واقتصادية ودبلوماسية وتكنولوجية وعسكرية، و كانت تلك العناصر ذات علاقة ترابطية فيما بينهما حيث يدعم كل منهما الأخر، حيث يؤدي الضعف في احدها الى ضعف العناصر الأخرى والعكس، وكانت الدول في السابق أكثر انعزالاً عن بعضها البعض، وكانت مسالة الدفاع عن حدودها القومية جزءا هاما من حماية عناصر قوتها القومية وجاء الفضاء الالكتروني بخصائص وعناصر مميزة ، وليكون له تأثيرعلى الأمن والاقتصاد الدولي[1]

وتحول الفضاء الالكتروني لأداة عالمية لتبادل المنافع والمعلومات والمشاركة في إنتاجها عالميا سواء من قبل الأفراد أو المؤسسات، وشكل ذلك خرقا للمفاهيم التقليدية الخاصة بفكرة القومية حيث تمدد الفضاء الالكتروني بشكل تجاوز الحدود التقليدية للدول وكذلك أجواءها الخارجية عبر الأقمار الصناعية، وفقدت الحكومات السيطرة على انسياب المعلومات والأفكار من وإلى الداخل، وأصبحت المعدات Hardware تتجه لان تصبح أكثر اندماجية في وظائفها وفي درجة تفاعلها كالكمبيوتر والتلفزيون والهاتف المحمول والأقمار الصناعية وشبكات الإنترنت، وأصبحت تلك الأدوات تعطي الفرصة لكل فرد

---

(1) James R. Hosek, **"The Soldier of the 21st Century,"** in New Challenges, New Tools for Defense Decisionmaking, ed. Stuart E. Johnson, Martin C. Libicki, and Gregory F. Treverton (Santa Monica, CA: RAND, 2003),p. 196.

حق الدخول والمساهمة والمشاهدة والتفاعل عبر شاشات الكمبيوتر، وأصبح الفضاء الإلكتروني يتسع لكافة أنحاء العالم في ظل تراجع دور الدولة سياسيا واقتصاديا وثقافيا وسيطرتها على مواطنيها مع السماوات المفتوحة والفضاءات التكنولوجية، وضعف احتكار الدولة للقيم الثقافية أو التعبير عنها أو حتى بث قيم الولاء.

وتشهد العديد من الدول عمليات خصخصة لمرافق كانت في السابق من المرافق الإستراتيجية بهدف تشجيع الاستثمار الأجنبي والقطاع الخاص إلا أن ذلك حمل معه مخاطر تتعلق بإمكانية تعرض تلك المرافق لهجمات، بعد ان أدي ذلك لخروج قطاعات كانت تعد في السابق من ركائز الأمن القومي من سيطرة الدولة، ويؤدي عدم وجود أي رقابة لتلك القطاعات من جانب الدولة الى ان تكون عرضة أكثر من غيرها للتعرض لهجمات إرهابية الكترونية، وبما يكون له تاثيرعلى الاقتصاد الكلي، وخاصة مع بروز فاعلين من غير الدول وتغير طبيعه الاعتبارات الجغرافية والجيوبوليتيكية مع التطورات في وسائل الاتصالات، وأصبحت البيئة الدولية الجديدة تفرض تغيرا على طبيعة الأولويات والضرورات الدولية. وتعلق الأمن الالكتروني بطريقة البحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ، ومن الناحية الفنية فإن المتخصصين يقصدون بأمن المعلومات بأنه الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن زاوية قانونية فإن أمن المعلومات هو محل دراسات فيما يتعلق بتدابير تأمين المحتوى الالكتروني ومكافحة أنشطة الاعتداء أو استغلال التقنية في ارتكاب جرائم معلوماتية ،ووضع تشريعات حماية المعلومات من الأنشطة غير المشروعة. ويتعرض الفضاء الإلكتروني لثلاثة أنواع من المخاطر منها ما يتعلق بالكوارث الطبيعية ومنها أخطار عامة والثالثة مخاطر الكترونية، ودخل الأمن الالكتروني ضمن الأبحاث والدراسات الإستراتيجية. وتمثل متطلبات توافر الأمن الالكتروني الدولي، اختبار سلامة الدفاعات الالكترونية، والتأكد من سلامتها وعدم تعرضها لأي خلل فني طارئ، وإن لا تعالج هذه المسألة كقضية منفصلة عن غيرها وإنما من ضمن ترسانة شاملة للدفاع تشكل إطارا رادعاً لأي حرب استباقية.(1)

ويتم تعزيز العنصر الوقائي ضد التعرض للهجمات عن طريق وجود شبكات إنذار في حالات الطوارئ فيما يتعلق بأوجه الانكشاف للفضاء الالكتروني والتهديدات والحوادث التي يتعرض لها. وإيجاد طابع تنظيمي أو مؤسسي حيث يتم إنشاء هيئات تتحمل المسئولية حول الحماية على المستوى الوطني والتنسيق مع الهيئات الحكومية أو المجتمع المدني أو القطاع الخاص أو العام. والبحث والتطوير فيما يتعلق بالجهود الدولية في استحداث البرامج الخاصة بالمكافحة والقدرة على الاستجابة واختبار خطط الإستراتيجية الأخرى، وفي حالة وقوع هجوم على هياكل البنية التحتية للمعلومات، وتعزيز البحث والتطوير على الصعيدين الوطني والدولي وتشجيع استخدام تكنولوجيا الأمن المستوفية للمعايير الدولية ومكافحة الهجمات التي تتعرض لها البنية التحتية للمعلومات والعمل عند الاقتضاء على كشف المعلومات الخاصة بهذا التقصي للبلدان الأخرى، وتمكين الدول من التحقق في الهجمات التي تشن على البنية التحتية المعلوماتية

(1) Amoroso, Edward G., **Cyber Security**. Summit, NJ, Silicon Press, 2007. p177 .

وتقديم مرتكبيها إلى القضاء وتنسيق هذه التحقيقات مع دول أخرى'ويتضمن تعزيز الأمن الالكتروني اتخاذ عدد من الإجراءات لعل أهمها :

أولا:- تحديد وتعريف القطاع الحيوي

وهو يشمل المنشآت والخدمات والتجهيزات الأساسية التي يحتاجها المجتمع، وتختلف الدول في تحديد ما قد يعد منشآت حيوية أو حرجة وكذلك في إيجاد تعريف واضح لها، فهناك دول لديها تحديد لما تعتبره بنية تحتية حيوية وتحديد الأمن الالكتروني مثل استراليا وكندا ونيوزيلندا وبريطانيا والولايات المتحدة، بينما هناك دول ليس لديها كذلك تحديد ما يمكن إن تتضمن القطاعات الحيوية في اغلب الدول على المؤسسات المالية والبنوك والخدمات الحكومية والاتصال وتكنولوجيا المعلومات وخدمات الطوارئ والإنقاذ والطاقة والكهرباء والخدمات الصحية والمواصلات والنقل والتموين والتوزيع ومحطات المياه، ويتم النظر إلى تلك القطاعات على أنها ثروة قومية ومنشآت تستحق الحماية وفق القانون الدولي، وتعرفها اللجنة الأمريكية للبنية التحتية الحيوية بأنها " شبكات مستقلة يعود ملكية معظمها في الدول المتقدمة إلى القطاع الخاص وهي تتضمن النظم والعمليات التي تعمل بصورة مترابطة ومنتظمة لضمان تقديم وتوزيع الخدمات والسلع الأساسية ."، فالبنية التحتية الحرجة عبارة عن إطار من الشبكات المستقلة والنظم المتوافقة مع عمل الصناعات والمؤسسات وتوزيع القدرات الخاصة بتدفق السلع والخدمات الأساسية اللازمة لتحقيق الأمن الاقتصادي والقدرة على الدفاع " (1)

ثانيا:- الطابع التنظيمي والمؤسسي الخاص

أصبحت مسئولية الأمن الالكتروني في معظم الدول أو حماية البنية التحتية الحرجة يختص بها أكثر من هيئة أو مؤسسة أو في إطار تعاون مع الأقسام المختلفة والفاعلين، وقد حدث هذا الاهتمام العالمي بعد أحداث الحادي عشر من سبتمبر ٢٠٠١ مع بروز ظاهرة الإرهاب الدولي، كما أدى تصاعد الأخطار التي تهدد البنية التحتية الحرجة إلى إنشاء المؤسسات والهيئات المختصة فهناك مثلا هيئة الأمن وخدمات الطوارئ بكندا، والمكتب الفيدرالي لأمن المعلومات بألمانيا، ومركز حماية البنية التحتية بنيوزيلندا، ومركز تسيق امن البنية التحتية القومية بالمملكة المتحدة، وهناك وزارة الأمن الداخلي بالولايات المتحدة، وفي استراليا هناك العديد من المنظمات لحماية امن البنية التحتية الحيوية من خطر التعرض للهجمات الطبيعية أو الالكترونية، واعتبر الأمن الالكتروني جزءا من جهود الدول لمكافحة الإرهاب ومن ثم فقد ضمت مجموعه حماية البنية التحتية الحرجة الاستخبارات والشرطة والدفاع لهياكلها.

وفي النمسا لا يوجد جهة مسئولة عن حماية البنية التحتية بل هناك اهتمام من كل الوزارات من خلال الإجراءات التي تقوم بها للحماية، وفي فنلندا يعد الأمن الالكتروني هو قضية امن البيانات والتي لها أهمية اقتصادية ترتبط بنمو وتطور مجتمع المعلومات، وهناك العديد من المنظمات التي تتعامل مع الأمن الالكتروني منها الهيئة المنظمة للاتصالات والطوارئ ومكتب الدفاع الاقتصادي ولجنة امن البيانات، وفي

(1) وقد حذرت الهيئة الدولية للطاقة الذرية من خطر تعرض المنشئات النووية لهجمات الفضاء الإلكتروني وخاصة أن تلك المنشئات تعتمد على تنظيم المعلومات وتكنولوجيا الاتصال والمعلومات وذلك بعد أن اخترق احد الفيروسات قاعدة "دافيس بس " النووية في ولاية اوهايو الأمريكية عن طريق اختراق شبكات الكمبيوتر الخاصة للمزيد:.

, Kevin Paulsen ,."UN warns of nuclear cyber attack risk" , Security Focus , 27-9- 2004.

فرنسا يتم النظر إلى الأمن الالكتروني على انه يعد قضية تختص بالجرائم عالية التقنية، بما يجعلها تؤثر على نمو مجتمع المعلومات وتقع مسئولية حماية الأمن الالكتروني على عاتق الأمانة العامة للدفاع الوطني.

وفي ايطاليا يتم النظر إلى الأمن الالكتروني على انه جزء من التقدم في مجتمع المعلومات، ولا توجد سلطة أو هيئة إيطالية تتعامل مع الأمن الالكتروني وإنما توجد فقط مجموعه عمل حول الأمن الالكتروني بوزارة التكنولوجيا والابتكار وتضم ممثلين من كافة الوزارات، وفي هولندا هناك العديد من الهيئات المعنية بحماية البنية التحتية الحرجة ولكنها تخضع لإشراف وزارة الداخلية والعلاقات الخارجية، وفي النرويج هناك هيئة الدفاع والتخطيط والطوارئ، وفي السويد هناك هيئة الطوارئ السويدية بداخل وزارة الدفاع كما إن هناك هيئات مشابهه في بعض الدول العربية كالسعودية والإمارات والبحرين والكويت ومصر وجاءت الجهود الدولية للحكومات وبالتعاون مع الخبراء ورجال الأعمال ومنظمات المجتمع المدني وذلك لان الملكية والتشغيل لتلك الأنظمة الحيوية يقوم بها القطاع الخاص والذي يتحمل الكثير من الأعباء لجعل تلك البنية التحتية أكثر أمنا، ومن ثم فان شراكة القطاع الخاص مع العام والحكومة الوطنية تعد محور أساسي في إستراتيجية مكافحة الإرهاب الإلكتروني وتعزيز الأمن الالكتروني.

ثالثا:- دور القانون والأطر القانونية:

على الرغم من أن العديد من الدول المتقدمة أصبح لديها الوعي بأهمية حماية امن المعلومات فإنها قد بدأت متأخرة في إعادة هيكلة أطرها التشريعية الخاصة بحماية الفضاء الإلكتروني بعد أحداث ١١ سبتمبر ٢٠٠١، وذلك لان القوانين الوطنية لم تتواكب مع التطورات التكنولوجية الحديثة، فهناك من الدول من اتجه إلى تحديث أطرها التشريعية بينما تمكنت دول أخرى من إصدار قوانين محددة حول الجريمة الالكترونية، وضمت تلك الإجراءات حماية البيانات والخصوصية والاتصالات وتعزيز متطلبات مجتمع المعلومات وحماية الهوية والتوقيع الالكتروني والتجارة الالكترونية، كذلك العمل على تحقيق التعاون والتوافق الدولي في مجال قانون مكافحة الجرائم الالكترونية بما يساعد على تحقيق معدلات عالية للحماية الخاصة بالبنية التحتية الأساسية للمعلومات. وركزت المعالجة القانونية على وجه النظر في الخطر كجريمة متمثلا في الجهود في مكافحة الجريمة الالكترونية، في حين إن القطاع الخاص رأى إن تلك القضية أو الخطر مشكلة محلية وتقنية ولها خسائر اقتصادية، ولكن مع انتشار مصادر الخطر أخذت تلك القضية الاهتمام الأكبر، وذلك لان التكنولوجيا عملت على انتشار الخطر وفي نفس الوقت أعطت إحساسا بان هناك صعوبة في مواجهه الهجمات المحتملة، وركزت الإجراءات على الطابع الوقائي ومحاولة الحد من الخسائر في حالة التعرض لمثل هذا الخطر، وأصبحت القواعد القانونية لها أهمية في وضع الاستراتجيات الخاصة بالمكافحة وتلعب دورا في الحد من دور الدولة الأمني وخاصة استخدام القوات المسلحة بما ينعكس على انتهاك الحريات المدنية، كما إن القانون وسعيه إلى تجريم تلك الهجمات من شأنه أن يمثل ضغطاً ومجالاً للتعاون مع الدول الأخرى، وهناك عوامل تحد من المواجهة القانونية، والتي منها نقص المعرفة بمسالة توظيف المؤسسات القانونية واختلاف الأنظمة القضائية بين الدول، وعدم تبني قوانين واضحة في بعض الدول، وعلاقة التعاون بانتهاك السيادة القانونية للدول.

رابعا:- البحث والتطوير:

أصبح هناك اهتمام عالمي بالبحث والتطوير في مجال الأمن الالكتروني ويتراوح هذا الاهتمام من الأبعاد التقنية إلى الأبعاد الاجتماعية، وتعد الولايات المتحدة والاتحاد الأوربي من اكبر الفاعلين في هذا المجال وذلك من خلال تعزيز التعاون مع مؤسسات البحث في الجامعات والمؤسسات التي تتبع القطاع الخاص والمعامل وشهادات الجودة ومجالس البحث الوطنية، وقد دفع البعد الدولي في عمل البنية التحتية الحيوية للمعلومات إلى نمو الاعتماد الدولي المتبادل وخاصة ما يتعلق بالأنظمة المعلوماتية المشغلة لها، وكذلك عبور تلك الأخطار للحدود التقليدية بما يعظم من خطر التعرض دوليا.

ويتطلب ذلك أن تشهد عمليات البحث والتطوير تعاونا دوليا وثيقا وذلك للزيادة العالمية في انتشار تكنولوجيا الاتصال والمعلومات واتجاه الأنظمة إلى المزيد من التعقيد ونمو الاعتماد المتبادل بين مكونات البنية التحتية الحيوية، وأصبحت المشكلات العالمية تتطلب حلولا عالمية أيضا من اجل العمل على تحسين الكفاءة وانخفاض التكلفة، وتحسين عمليات الدخول إلى البيانات المتعلقة بعملها والتي تصبح غير متاحة على الصعيد الوطني. وهناك حاجة للمزيد من البحث بطرق منهجية لتحليل البنية التحتية للمعلومات والقضايا الأخرى المتعلقة بها كطبيعة عملها وتحديد قطاعاتها الحيوية ودراسة قابليتها للتعرض للأخطار وتأثير ذلك على أمنها، ويمكن أن يتم ذلك من خلال التكامل ما بين مجموعه الأدوات والطرق الخاصة بالتحليل والإجراءات الوقائية وعملية صنع القرار وبما يتطلب رؤية شاملة لمواجهه الخطر الذي يتنقل من الطابع الافتراضي إلى الطبيعي لحماية البنية التحتية للمعلومات.

## المطلب الثاني:
## الفضاء الإلكتروني وخصائص المرفق الدولي والتراث المشترك للإنسانية

لا يخضع الفضاء الالكتروني للسيطرة أو التحكم من جانب طرف اللهم إلا خضوع عملية إدارة الإنترنت إلى منظمة ايكان الأمريكية وهي منظمة غير حكومية، فالفضاء الإلكتروني يتجاوز الحدود والمناطق الجغرافية كما إن المهاجمين في الفضاء الإلكتروني يتجاوز حدود الجنسية مع تسهيلات الدخول إلى الشبكة الدولية للمعلومات، ويعد مفهوم السيادة من أحد المفاهيم التقليدية العامة التي قام على أساسها القانون الدولي والعلاقات الدولية، ولكن هذا لا يسري بصورة مباشرة مع تكنولوجيا الاتصال والمعلومات والشبكات الخاصة بها التي تكون ما يطلق علية بالفضاء الإلكتروني، ويعد الفضاء الإلكتروني لما أصبح علية من أهمية إستراتيجية دولية، وتمثل عملية الحافظ على أمنه مطلباً دولياً باعتباره مرفقاً دولياً يمكن إن يتم التعامل معه كما تعامل القانون الدولي مع المرافق الدولية كالتعامل مع البحار والقارة القطبية والفضاء الخارجي وهذه المناطق تعد خروجا عن نظام ويستفاليا وما يتعلق من مفهوم السيادة كأساس للعلاقات الدولية.

و يخضع المرفق الدولي لاستخدام كل البشرية في إطار التراث المشترك للإنسانية، وإذا ما اتسعت تلك المبادئ لتشمل الفضاء الإلكتروني فانه يواجهها بعض التحديات التي يمكن التغلب عليها والتي تنجم من اختلاف خصائص الفضاء الإلكتروني عن تلك الفضاءات الدولية، ويتميز الخطر الالكتروني بأنه غير متماثل وغير مرئي ويحمل في طياته خطر تعرض المقدرات الاجتماعية والأساسية لواحد أو أكثر من الدول

لمثل ذلك الخطر ومن ثم تكون المشكلة عالمية ولا يمكن حلها بجهود فردية أو حتى على المستوى الثنائي أو الإقليمي حيث إن الفضاء الإلكتروني لا يعرف الحدود التقليدية ولا يلقي لها بالا.

ويمكن للمهاجمين أن يعبروا الحدود الدولية في ظل العالم الالكتروني، وهذا ما يتطلب جهودا مشتركة من قبل جميل الدول على المستوى القانوني والتكنولوجي والسياسي والاقتصادي، وأصبح الأمن الالكتروني قضيه عالمية، مع ارتباطه بالمصلحة القومية للدول فرادى وللمجتمع الدولي ككل، ومثل ذلك سمة أساسية في مجال دفع مسالة إقامة مفاوضات دولية بشان التعامل مع الفضاء الإلكتروني والبحث عن قانون دولي يقدم معالجة شاملة لحدود وواجبات وحقوق استخدام الفضاء الإلكتروني، ليصبح الفضاء الإلكتروني جزءا من التراث المشترك للإنسانية ويتبع ذلك أن يكون الاستغلال والاستخدام من كافة الدول حقاً شرعياً لها.

ولقد حوي القانون الدولي تنظيما قانونيا عرف بنظرية الفضاءات الدولية والتي شكلت اللبنة الأولي في تأسيس نظام قانوني خاص بالفضاء الخارجي والقارة القطبية المتجمدة وأعالي البحار، وجاء مفهوم "الملك العالمي المشترك" ليعبر عن المنفعة الكلية لكافة ساكني العالم، ويعد مصطلح التراث المشترك للإنسانية حسب تصورات القانون الدولي بكل ما لا يخص أحدا كأعالي البحار أو كل ما يخص الجميع كمجال الذبذبات الإلكترون- مغنطيسية. كما يحيل المفهوم في السياق ذاته على ما هو عمومي، والحقيقة أنه كان من الممكن اعتبار "الملك العالمي المشترك" كذلك، لو كان ثمة شكل من أشكال التدبير القادر على تبين حقيقته وحمايته.

ومثلت فكرة التراث المشترك للإنسانية فكرة هامة توصل إليها المجتمع الدولي وذلك تحت ضغوط المتطلبات الاقتصادية والاجتماعية والسياسية التي يطالب بها المجتمع الدولي وكانت احد أوجه التطور الحديث للقانون الدولي، بعد إن كان مقصوراً على مجرد حكم وتنظيم العلاقات بين الدول، ويتكون مبدأ التراث المشترك للإنسانية من أعمدة رئيسية يقوم عليها وهي انتفاء الملكية وتحقيق صالح الإنسانية جمعاء، والمشاركة العادلة في الفوائد والإدارة المشتركة من خلال جهاز دولي، وان يتم تحفيز الاستخدامات السلمية وحدها وان خلق ملك مشترك يجب أن يتم بإسهام الجميع في التكاليف والاستفادة من العوائد بصورة متساوية ، ويمثل ذلك " المنفعة العليا العالمية" وتوجد علاقة بين "الارادة العامة" والملك المشترك والتي تعني القرار الجمعي الذي يهم مصلحة المجتمع برمته في مقابل الرغبات الفردية وتجسد الإرادة العامة مصالح الإنسانية،

وأثار ظهور الفضاء الإلكتروني كظاهرة جديدة في العلاقات الدولية مسألة كيفية التعامل معها وتنظيمها لخدمة الأهداف الإنسانية السلمية والعمل على الحد من الاستخدام غير السلمي له كاستخدامه في المجال العسكري أو شن عمليات إرهابية أو بث الكراهية الدينية والعنصرية، ومن ثم أصبح هناك حاجة وضرورة ملحة لفتح أفاق جديد لتطبيق مبدأ التراث المشترك للإنسانية على هذا المجال الحيوي والاستراتيجي للبنية التحتية الكونية للمعلومات وللحيلولة دون تحول الفضاء الإلكتروني إلى منطقة نزاع دولي.

ويعد الفضاء الإلكتروني في حقيقة الأمر أوسع من الإنترنت حيث يعبر عن وجود مكان أو محيط ما يجتمع من خلاله حركة تفاعلات بين وحدات النظام الدولي، حيث يتم تلاقي كافة الرسائل وصفحات الإنترنت والتي تم إرسالها من قبل أي فرد لكي يراها ويتفاعل معها أي فرد في العالم، وانه وفقا للتعريف القانوني للمنطقة التي يطلق عليها "تراث مشترك للإنسانية " فإن الفضاء الإلكتروني يعد جزءاً من ذلك التراث حيث يشكل مصلحة دولية وعالمية يصبح من خلالها العالم بحاجة إلى تنظيم حركة التفاعلات داخل تلك الظاهرة بما يضمن الحفاظ على الاستخدام السلمي له، حيث يجمع الفضاء الإلكتروني مع غيرة من الفضاءات الدولية عدم وجود حدود جغرافية أو امتداد لسلطة المحاكم الوطنية علية أو وجود سلطة خارجية تتحكم به تحكما كاملا[1].

ومن ثم فان تلك المبادئ والخصائص التي أوجدت فضاءات دولية تنطبق على فكرة الفضاء الإلكتروني ولكنة يختلف بسبب عدم وجود قواعد واضحة إلى الآن تتحكم به وتنظمه، وربما يرجع ذلك إلى طبيعة تلك الظاهرة الجديدة في العلاقات الدولية من ناحية والى سرعة التطور العلمي والتكنولوجية والتي سبقت بكثير درجة التطور في الأطر القانونية الدولية الحالية، وكذلك عدم وجود قواعد قانونية واضحة تتعامل مع تلك الظاهرة وذلك على الرغم من التقدم الذي أحدثته عدد ليس بقليل من الدول على مستوى العالم في التعامل مع تلك الظاهرة، وظهر اختلاف في التوصيف القانوني لهجمات الإرهاب الالكتروني في إطار القوانين المحلية، والتي بحاجة إلى تفعيل التعاون الدولي في مواجهه تلك الظاهرة.

وأصبحت البنية التحتية الكونية للمعلومات ذات أهمية عالمية على المستوى الاقتصادي والسياسي والثقافي والاجتماعي وإن وحدة الإنسانية لا يمكن بأي شكل من الأشكال أن تتأسس على وحدة الدين أو الفلسفة أو السلطة، بل يكمن شرط تحققها أساسا في التعددية، وهو شرط يبدو من الصعب ضمان ديمومته في عصر يتسم بهيمنة التجريد بحكم سيادة المجال الرقمي، وبناء على ذلك، يتجلى التحدي الذي يجب رفعه لمواجهة عولمة التجريد والسوق في تحقيق ديمومة الاعتراف بالآخر والتعدد. وفي تجاوز المفارقة الناتجة عن توظيف التقنيات المعلوماتية القائمة على التنميط وذلك في إطار تحقيق الاختلاف[2].

ويطرح مجتمع المعلومات العالمي، بشكل حقيقي وبيّن إشكالا سياسيا عاما. ويكمن في تحديد مفهوم "الملك العالمي المشترك" وفي حصر المستفيدين من مجتمع المعلومات ودور الثورة المعلوماتية على مستوى تعميق التفاوتات الاقتصادية والاجتماعية والثقافية بين الأغنياء والفقراء، ثم في تباين المستوى "الحضاري" للعولمة ارتباطا بمجتمع المعلومات. ويفرض الحسم في كل ذلك تملك معايير لتقييم الملك المشترك وقد سعى المجتمع الدولي إلى حماية التراث المشترك للإنسانية ومنها اتفاقيات جينيف ١٩٤٩ وبروتوكولاتها الإضافيين، واتفاقية لاهاي لحماية الممتلكات الثقافية في حالة النزاع المسلح لسنة ١٩٥٤، وكذلك اتفاقية باريس الدولية بشان التدابير الواجب اتخاذها لحظر وبيع استيراد وتصدير ونقل ملكية الممتلكات الثقافية بطرق غير مشروعه، كما إن هناك اتفاقية باريس الدولية لحماية التراث العالمي الثقافي والطبيعي وفي إعلان

---

(1) Darrel C. Menthe*," **Jurisdiction In Cyberspace: A Theory of International Spaces**",4 Mich. Telecomm. Tech. L. Rev. 69 (1998) available *at* (http://www.mttlr.org/volfour/menthe.pdf)

(2) فيليب كيو "من الملك العالمي المشترك إلى عصر المعلومات" ترجمة " حسن الوزاني "، مجلة فكر ونقد ، العدد ٢٩ ،٢٠٠٦ (http://www.fikrwanakd.aljabriabed.net/n29_06wazzani.htm)

مبادئ التعاون الثقافي الدولي والتي تم إعلانها في ٤ نوفمبر ١٩٦٦ حيث اوجب الإعلان الاحترام والمحافظة على كل ثقافة، حيث إن الثقافات جميعها بما تحمله من تنوع وتباين جزءا من التراث المشترك للإنسانية، و كما دعا الإعلان إلى إسهام وسائل الأعلام في دعم السلام والتفاهم الدولي.(1)

وهذا ما يحتاج إلى تفعيل دور الأمم المتحدة لفرض "ملك عالمي مشترك"، يعبر عن مصالح المجتمع الدولي حيث إن الدول تكون اضعف في سبيل فرض هذا الملك المشترك. وأصبح يستخدم الفضاء الإلكتروني بصورة متزايدة بما يهدد المصالح الحيوية عن طريق استخدام أسلحة الفضاء الإلكتروني سواء للقيام بعمل إرهابي أو المساعدة في القيام بعمل عسكري تقليدي، وهذا ما يعد انتهاكا لمبدأ حظر استخدام القوة في العلاقات الدولية الوارد في المادة ٢فقرة ٤ من ميثاق الأمم المتحدة والذي يتعامل مع تهديدات تقليدية بما يجعل هناك ضرورة ملحة لإدماج التهديد الذي يمثله الإرهاب الإلكتروني ضمن تفسير تلك المادة باعتبارها نوعا من استخدام القوة في العلاقات الدولية ويمثل تهديدا للسلم والأمن الدوليين، حيث يستخدم الفضاء الإلكتروني إما كوسيط للعمليات العدائية أو الصراعية أو إن يتم استخدامه كأداة للهجوم، مع اعتبار إن استخدام الدول للفضاء الالكتروني لا يعد انتهاكاً لسيادة الدول الأخرى بالمعني القانوني، وإنما قد يقترب من حالة استخدام الدول المجال الجوي للدول الأخرى في الملاحة الجوية.(2)

وجاء ذلك مع بروز مخاطر محلية وعالمية في ذات الوقت حيث إن الخطر المحلي يصبح عالمياً من خلال شبكات الاتصال والمعلومات حيث أصبح العالم أكثر ترابطا واعتمادا على شبكات الاتصال والمعلومات وأصبح هناك عالم يشبه القرية الصغيرة، بما يمكن إن يتحول خطر محلي من خلال مصدر محلي إلى حدث دولي له آثار دولية. كما إن عملية تحديد الدولة التي تقع تحت ذلك العدوان مسالة هامه من اجل تحديد المسئولية القانونية وراء تلك الهجمات، وهذا الأمر يصبح صعبا بالإضافة إلى تشعب مصادر الهجوم وتداخله كما إن الفاعلين من غير الدول قد يكونوا مصدراً لتلك الهجمات وليست الدول ذات الشخصية القانونية الدولية.

كما إن التعامل مع الفضاء الإلكتروني من خلال مبدأ السيادة غير كاف، بل يجب النظر إليه ككيان أو مجال واحد ووحدة متكاملة في إطار اعتباره مرفقاً دولياً كتلك التي تم إقرارها من جانب المجتمع الدولي في إطار مبدأ التراث المشترك للإنسانية، ويصبح تأمين الفضاء الإلكتروني مسئولية دولية من كافة أطراف مجتمع المعلومات العالمي، و يستلزم ذلك تعاونا وإستراتيجية مشتركة للتعاون ضد الأخطار التي يمكن أن يواجهها الفضاء الإلكتروني، كما أن مسالة احترام سيادة الدول قد يكون لها دور أيضا في قيام الدولة بدورها في تعزيز الأمن كطرف حيادي كما إن تلك الدولة يمكن أن تمارس سلطتها في دعم عملية دفع الجهود الوطنية والدولية لتنظيم استخدام الفضاء الإلكتروني، وهذا ما يتطلب أيضا تحديد ماهية تلك الاستخدامات وما يمكن أن ينطوي على استخدام القوة في العلاقات الدولية ويعد هجوما مسلحا وكما ورد في ميثاق الأمم المتحدة.

---

(1) د. امين احمد الحذيفي، " الحماية الجنائية للاثار "، دراسة مقارنه، دار النهضة العربية، القاهرة، ٢٠٠٧ ص ص ٢١٢ ـ ٢٢٥.

(2) Scott J. Shackelford," From Nuclear War to Net War :Analogizing Cyber Attacks in International Law", **Op.Cit**, pp 20-24.

## المطلب الثالث:
## نحو اتفاقية دولية للفضاء الالكتروني
## وتعزيز اطر القانون الدولي الحالي

أصبحت قضية امن الفضاء الالكتروني قضية دولية تحظي بالمزيد من الاهتمام المتصاعد وذلك يرجع إلى تشعب تلك القضية وارتباطها بكافة مجالات الحياة وكونها تحمل عدة أبعاد لعل يتمثل أهمها : اولا : البعد السياسي بعلاقة الأمن الالكتروني بالأمن القومي وبقضايا التنمية الاقتصادية والاجتماعية والاستقرار السياسي، كما إن الأخطار المرتبطة بتكنولوجيا الاتصال والمعلومات تمثل تهديدا للدول والمنظمات السياسية والمواطنين بما يفرض الحاجة لوجود حماية شاملة على المستويات المحلية والإقليمية والدولية، وأهمية وجود دور لكل أطراف المجتمع المعلوماتي، والعمل على تحديد الإجراءات العامة التي يجب أن تتخذ بما يتواكب مع الأمن والحماية اللازمة لنمو الثقة في بيئة تكنولوجيا الاتصال والمعلومات

وثانيا البعد القانوني وهو البعد الخاص بدور القانون في عملية تعزيز الأمن وما يتطلبه من فهم عالمي للقضايا القانونية التي تتعلق بتكنولوجيا الاتصال والمعلومات وسوء استخدامها، وهذا ما يتطلب وجود أطر قانونية على المستويات الوطنية والدولية، وأن يتم ترجمة الجهود الدولية لقواعد قانونية وتطوير نموذج عالمي لاتفاق دولي، والفهم المشترك للجرائم المرتبطة بالكمبيوتر والإنترنت والتعامل مع الأخطار الالكترونية .

وثالثا : البعد التنظيمي بوجود هيكل تنظيمي أو مؤسسي يعمل على تحديد الأخطار ودعم عملية الأمان وإدارة وتنسيق إجراءات المكافحة وتحديد معايير للأمن وتحديد المرافق الإستراتيجية والحيوية والعمل على صياغة إستراتيجية أمنية واضحة والقدرة على الاستجابة في وقت الطوارئ ،وإدارة أزمات الأمن في بيئات متحركة ومعقدة ،والاستفادة من الخبرات الممكنة في تدريب العنصر البشري ووجود قدر من المسئولية والمحاسبة والشفافية . ورابعا : البعد التكنولوجي فيما يتعلق بفهم الإمكانيات والقدرات التقنية لتكنولوجيا الاتصال والمعلومات والاستخدام السيئ لها وفهم الأخطار المرتبطة بها وكيفية الاستجابة تكنولوجيا لتلك الأخطار، والعمل على تصميم برامج حماية وأدوات أمنية فاعلة بما يساعد على وجود درجات التكامل والثقة في البنية التحتية للمعلومات والخدمات الالكترونية.

وخامسا : البعد الاجتماعي: يكون دور الأفراد في عملية الأمن هامه بمعرفتهم بالإجراءات الأمنية التي يمكن أن تستخدم لتأمين مصادر المعلومات وتكنولوجيا الاتصال والمعلومات، و معرفة أنواع تلك الأخطار وتداعياتها، وهذا ما يساعد على بناء ثقافة عالمية للأمن الالكتروني يرتكز على المعرفة الجيدة بالمعايير الدولية والتوصيات الخاصة بالأمن، ويعد تقوية دور الموارد البشرية هاماً من خلال التعليم والخبرات والتدريب وبناء قاعدة علمية قادرة على التعامل مع تلك الأخطار ورفع الوعي العام.

وتمثل تلك الأبعاد مقدمة لكيفية التعامل مع ظاهرة الفضاء الالكتروني وكيفية تأمينها من المخاطر كظاهرة الإرهاب الالكتروني واستخدام القوة المهدد للأمن والاستقرار الدولي. بعد أن أصبح الفضاء الإلكتروني كظاهرة لها تأثير على كافة المجالات وزادت أهمية المعلومات ودورها في القوة العسكرية التقليدية وفي تشكيل الإستراتيجية والمفاهيم الحديثة وظهر التفوق المعلوماتي " كأحد مفاتيح النصر [1]

---

[1] Michael N. Schmitt," , War, Technology and the Law of Armed Conflict", International Law Studies, Volume 82, Naval War College Newport, Rhode Island 2006,pp 137-166

وينصب الاهتمام العسكري على أهمية البعد التكنولوجي للصراع كإحدى أدوات تعظيم القوة والتفوق، وفي نفس الوقت أصبح هناك فاعلون على نطاق متسع يمكنهم الاستحواذ على أدوات القوة وتجميعها وإنتاجها، وأصبح هناك درجات عالية من التنافس حول السيطرة والابتكار والتحكم في المعلومات التي يلعب شبكات الاتصال والمعلومات دورا محوريا في هذا التطور مع العولمة والانتشار الضخم لها عالميا، وأتاح الفضاء الإلكتروني لفاعلين من غير الدول القدرة على الحصول على قدرات تمكنهم من تعظيم قوتهم وزيادة نفوذهم وتأثيرهم ليس فقط على نطاق محلي بل على نطاق دولي أيضا.

وظهرت العلاقة ما بين الفضاء الالكتروني والصراع كبعد جديد يتضمن كل شبكات الاتصالات ومصادر المعلومات التي يتم تبادلها الكترونيا.(1) وأصبح هناك قواعد للقانون الدولي ما ينطبق مباشرة على أنشطة الفضاء الإلكتروني وهي المبادئ المعمول بها بين الأمم ومبادئ القانون الدولي الناشئة عن القانون الدولي العرفي والمعاهدات، والمبادئ العامة التي استندت عليها الأمم المتحضرة كالقواعد التي تحكم اللجوء لاستخدام القوة وقواعد التسوية السلمية للمنازعات الدولية والقواعد المحددة لقواعد الدفاع عن النفس، والقواعد المتضمنة في ميثاق الأمم المتحدة والنظام الأساسي لمحكمة العدل الدولية والقانون الدولي الإنساني، وهناك نوعان من القواعد القانونية الأول تعمل على إشباع الحاجات والمصالح العليا والمشتركة للمجتمع الدولي ككل وهي قواعد مطلقة في تطبيقها.

وهناك أيضا القواعد النسبية التي تنظم حقوق وواجبات الدول فيما بينها ولا تسري إلا فيما يتعلق بهذه الحقوق أو تلك الواجبات. وتطرح طبيعة هجمات الفضاء الإلكتروني مدى إمكانية تطبيق القواعد القانونية الدولية التي تنبثق من ميثاق الأمم المتحدة تساعد على المعالجة القانونية أو إن الأطر القانونية ليست كافية للتوصل إلى حلول تعالج معضلة الأمن التي تفرضها هجمات الفضاء الإلكتروني. وهناك وجهتا نظر الأولى ترى إن هناك حاجة إلى وجود إطار قانوني جديد كليا، أو أن يتم الاقتصار على تبني النظم القانوني القائمة فقط، وان أفضل طريقة لضمان معالجة شاملة تكمن في وجود اتفاق دولي يتعامل بالتحديد مع الأمن الالكتروني وكيفية وضعه وطريقة معالجته في القانون الدولي. وتطرح كيفية إنشاء بيئة قانونية تنظر إلى العدوان الالكتروني باعتباره إخلالا جسيماً بالنظام القانوني ومرادفاً للجريمة الدولية المنظمة أو عدواناً ضد دولة أخرى، وتدفع عملية الضرر المتوقع والمتخيل في حالة التعرض لهجمات الفضاء الإلكتروني إلى إثارة الجدل بشأن إمكانية تطبيق ما أرساه القانون الدولي الإنساني من قواعد تعمل على الحد من استخدام القوة أو التهديد بها أو حتى تنظيم استخدامها في حالة الصراعات المسلحة الدولية وغير دولية الطابع بهدف حماية المدنيين والمنشآت المدنية والإمكان التي تستحق حماية خاصة أو المنشآت التي تحتوي على خطورة خاصة.

وتصبح الخطر ليس فقط، لمصالح الأمم أو لجماعات الضغط. وإن الخطر الأساس الذي يمكن أن ينتج عن "الحضارة العالمية" يكمن في الحد من التعدد ومن إمكانيات الاعتراف بالآخر وذلك من خلال تنميط أشكال التعامل. وبمعنى آخر، إن تحقيق الشفافية وتسهيل تداول المعلومات على المستوى العالمي يتم على حساب الاختلاف والتعدد فمستوى حضارة ما من خلال درجة احتوائها لما لا يمكن توقعه. إن وحدة

---

(1) Myriam A. Dunn," The Cyberspace Dimension in Armed Conflict", Information and Security, An International Journal, Vol. 7, 2001, pp. 145-158

الإنسانية لا يمكن بأي شكل من الأشكال أن تتأسس على وحدة الدين أو الفلسفة أو السلطة، بل يكمن شرط تحققها أساسا في التعددية. وتبقى مسائل التعاون الدولي أهمية بالغة، أبرزها الاتفاق في حقل الاختصاص القضائي والقانون الواجب التطبيق في بيئة النزاع في الفضاء الالكتروني، وهذا ما يتطلب معرفة الأسس التي يتعين إن يتم التفكير فيها في كل نشاط يهدف إلى تنظيم ضروري للفضاء الالكتروني، والاهم أن يكون تنظيما يراعي هذه السمات التقنية وهذه الخصائص والمميزات التفاعلية اللامتناهية [1].

ويعبر الفضاء الإلكتروني من دولة لدولة ومن منطقة إلى أخرى، ومن جهة عمل إلى أخرى دون قيود وبكل اللغات مع التداخل بين الشبكات المحلية والإقليمية والدولية، وفي هذا الانتقال يتم المرور عبر مناطق الاختصاص القضائي ومناطق السيادة في العالم ،وهذه المناطق قد لا يكون بينها تعاون أو حتى روابط، ففي مثل هذه البيئة ثمة حاجة لجهد استثنائي على النطاق الدولي أهم ما يتعين إن يتصف به الخروج من الأطر والمفاهيم التقليدية التي بني عليها القانون الدولي، والعمل على اتخاذ تدابير ملاءمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود، أو ذات الطبيعة الدولية ووجود اتفاقيات دولية تنطوي على نصوص تنظيم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، والأشكال الأخرى للمساعدة المتبادلة، مع كفالة الحماية في الوقت نفسه لحقوق الأفراد والدول.

وتعد التعاملات المرتبطة بتقنية المعلومات كغيرها من مجالات الحياة يجب أن تخضع للأحكام المستمدة من القانون الدولي والعرف يكفل وضع الحقوق والتزامات الأطراف المختلفة والموقف من القضايا المختلفة وفض النزاعات الناتجة عنها وتعد مسالة حماية البنية التحتية الكونية للمعلومات من ضمن أسس الأمن الدولي الجديد وما يتطلب ذلك من توافر قاعدة للتعاون الدولي المشترك وتحديد ماهية تلك القطاعات الحيوية وتوفير نظم حماية منتظمة لها ودعم مواجهه الأخطار التي يمكن أن تتعرض لها على المستوى التشريعي والسياسي والاجتماعي والاقتصادي، وأهمية دور الفضاء الإلكتروني في عمل البنية التحتية وما يستلزم من أهمية تعزيز الاستخدام السلمي له.

وكان المجتمع الدولي قد بذل العديد من الجهود للعمل على حظر استخدام أسلحة الدمار الشامل والتقدم في شأن المناطق الخالية من السلاح النووي. وكما كانت العلاقة حميمة بين الأسلحة والتقدم التكنولوجي فإنها أفرزت ثورة في الشئون العسكرية، وكان من ضمن ذلك ظهور أسلحة الفضاء الإلكتروني والتي أصبح لها إضرار سواء من خلال تهديدها لأمن الفضاء الإلكتروني أو سعي الدول وغير الدول إلى تطويرها واستخدامها وانتشارها، بما يعيد إلى الأذهان الجهود الدولية لحظر أسلحة الدمار الشامل، وأصبح هناك إمكانية لتوظيف تلك الأسلحة التي تختلف عن الأسلحة التقليدية. وبرزت تهديدات تلك الاستخدامات على الطابع المدني للفضاء الالكتروني إلى الحاجة إلى تضافر الجهود الدولية من اجل العمل على تعزيز الأمن والحماية لدور الفضاء الإلكتروني الايجابي على السيادة الدولية.

---

(1) للمزيد حول إعلان الدوحة يمكن الإطلاع علية على الرابط التالي أخر زيارة (١٢-٧-٢٠٠٧) (www.ituarabic.org/2008/CIIP/Doha_Declaration.pdf)

وكان من ضمن تلك الجهود الدعوة إلى اتفاقية دولية للحد من التسلح داخل الفضاء الإلكتروني مثل تلك الاتفاقيات التي تم انجازها في مجال الانتشار النووي والكيماوي والبيولوجي، حيث يمكن إن تساهم مثل تلك الاتفاقيات في حال تطبيقها على الفضاء الإلكتروني والأسلحة التي يمكن إن تستخدم من خلالها أن يتم وضع قيود على استخدامها وتوزيعها وانتشارها وتطويرها. كما يمكن أن تخضع تلك الانتهاكات إلى القانون الجنائي الدولي ومحكمة العدل الدولية ، ولكن ذلك يتطلب موافقة الدول ولكن تواجه عملية الدعوة إلى مثل تلك الاتفاقيات بعدد من التحديات حيث إن الدول قد ترفض الموافقة على أساس إن هذه القيود من شأنها أن تعمل على الحد من قدرتها على تطوير الأسلحة الهجومية، وفي نفس الوقت يحد من قدرتها على الدفاع في حال التعرض لهجوم الكتروني من دول أخرى أو فاعلين آخرين، كما إن ذلك الاتفاق يشمل فقط الدول في حين إن عملية استخدام أسلحة الفضاء الإلكتروني يمكن إن تأتي من أطراف من غير الدول كالمنظمات الإرهابية والإجرامية والتي لا تخضع لمثل تلك القيود.

و إن تلك القيود التي قد تفرضها الاتفاقية على الدول من شأنها أن تعظم من قدرة الفاعلين من غير الدول في استخدام تلك الأسلحة مقابل قدرات الدول.وهناك صعوبة في وضع الدول تحت الرقابة الفنية حول قدرتها على تطوير أسلحة الفضاء الإلكتروني، وصعوبة في معرفة مصادر الهجمات إن وقعت وتحديد المسئولية بشأنها ، ويمكن أن تتعرض دول إلى اعتداء أو هجوم صادر من أجهزة حكومية في دولة أخرى، ولكن قد يحرك تلك الهجمات طرف ثالث يمكن أن يسيطر على تلك الأجهزة، وتتميز تلك الأسلحة بقدرتها الهائلة على الانتشار عبر الفضاء الالكتروني ، ومن ثم فإن نموذج منع الانتشار الخاص بالأسلحة النووية قد لا يصلح كنموذج للتعامل مع الأسلحة في الفضاء الإلكتروني ذلك لأن انتشار التكنولوجيا أصبح عالميا في المجتمع الدولي ومن ناحية أخرى أصبح هناك صعوبة الفصل بين الاستخدام المدني والآخر العسكري.

و إن تحقيق الأمن الالكتروني الجماعي الدولي ومتطلبات إقامته يتطلب أن يوجد إيمان وثقافة عالمية بان السلام أمر غير قابل للانقسام أو التجزئة، وضرورة اتساع نطاق عضوية الدول فيه وان يكون ذلك النظام حياديا وموضوعيا، وان توجد قوة رادعه عسكرية لردع المخالفين لذلك النظام، كما ينبغي أن يتركز على الناس وليس حول الدول بالضرورة وهناك حاجة لوجود هوية إنسانية عالمية مع احترام حرية الأفراد في أن تكون لهم هويات وانتماءات متنوعة و ضرورة تشكيل تحالف عالمي لتعزيز السياسات المؤسسية التي تربط ما بين الأفراد والدول. ولكي يتم خضوع الفضاء الالكتروني للقانون الدولي يحتاج إلى تغيير تنظيمي قانوني وسياسي وامني وثقافي شامل.

وانه لكي يتم التوصل الى اتفاق دولي يجب ان يتم اطلاق حوار دائم حول ما يعد جريمة وإرهابا وما يمكن أن يدخل ضمن الاستخدام السلمي وأن يتم التمييز بينهما، وهذا الحوار يمكن أن يتقدم على جبهتين الأولى: طبيعة الهدف الذي يمكن أن يدخل ضمن ضوابط وقواعد قانونية وذلك لأنه يمثل أهمية ومعاناة لغير المحاربين كالهجوم على محطات الطاقة، أما الجبهة الثانية فهي طبيعة الأهداف التي تخرج على الأطر القانونية والتي تصبح في حاجة إلى الحماية حيث تكون إصاباتها غير معروفة ولا يمكن التنبؤ بنتائجها وكلها تسبب في حدوث معاناة

ومن ثم فانة لكي يتم التوصل إلى نظام قانوني دولي يحكم ظاهرة الفضاء الالكتروني،يجب ان يتم تحديد أولا: ماهية وكيفية التغلب على العمليات العسكرية باستخدام هجمات الفضاء الإلكتروني،وثانيا أن تكون الاتفاقية قادرة على تحقيق التوازن بين مبدأين أساسيين هما الأول: مبدأ الضرورة العسكرية والثاني احتمالية الوقوع، وثالثا:التمييز بين الأهداف العسكرية والمدنية ورابعا التصديق على هذه المعاهدة ضمن المحكمة الجنائية الدولية، و إن تفعيل القانون الدولي لكي يتلاءم مع تلك الظاهرة ويحكم حركة تفاعلاتها يجب إن يستند إلى: أولا: وسائل المنع أو الوقاية التي تستخدم في تطبيق أحكام القانون الدولي لصالح الضحايا أو يتم تطبيقها تطبيقا سليما، ثانيا: وسائل للرقابة وهي وسائل الأشراف المتواصل بما يتضمن الالتزام السليم عند تطبيق الأحكام التي تتكفل بمصلحة الضحايا، و ثالثا: العقوبات وهي جزء لا يتجزأ من أي نظام قانوني سليم وذلك بسبب قيمتها الرادعة، ورابعا: ضرورة البحث عن وسائل أخرى غير الطرق القانونية كالمكافحة الأمنية والثقافية.

# الخاتمة

# "نحو تعزيز دور الفضاء الالكتروني في دعم السلم الدولي "

## الخاتمة:

## نحو تعزيز دور الفضاء الالكتروني في دعم السلم الدولي

تكون لدى الباحث عبر استعراض فصول دراسته الخمسة هي مكونات هذه الدراسة عدد من النتائج والملاحظات التي تعلقت بفرضيات دراسته التي يمكن ابراز أهم ملامحها على النحو التالي:

فقد لاحظت الدراسة من - ناحية أولى- عن انه كان وما يزال للثورة التكنولوجية دوراً في تسريع وتيرة التغير في كل أبعاد الحياة داخل المجتمع الدولي، وما كان لذلك من دور في تغير طبيعة وبيئة العلاقات الدولية وأطرافها وعناصر القوة والصراع والأمن وحركة التفاعلات وحجم الفاعلين داخل النظام الدولي، وتحولت البيئة الدولية إلى بيئة يلعب بها المعلومات والمعرفة والأفكار مصدرا استراتيجيا للقوة على كافة مستوياتها السياسية و الاقتصادية والعسكرية.

وأصبحت ظاهرة الفضاء الالكتروني تشهد نشاطا مميزا عن النشاط الذي يمارسه الإنسان في باقي المجالات الأخرى كالبر والبحر والجو والفضاء الخارجي، وأصبح له دور فاعل في التأثير بدرجة أو بأخرى على تغيير طبيعة القوة ومصادرها واستخدامها في العلاقات الدولية وأيضا كوسيط في تقديم الخدمات المدنية في مجالات الاتصالات وخدمات الطوارئ والصفقات المالية والتجارة وخدمات الحكومة الالكترونية وفي عمل البنية التحتية الكونية للمعلومات والتي يتزايد الاعتماد الدولي عليها ، وارتقى ذلك التطور ليصبح للفضاء الالكتروني دور وأهمية إستراتيجية تجري به كافة تفاعلات ومصالح المجتمع الدولي قاطبة على الصعيد الاقتصادي والسياسي والثقافي والأمني والاجتماعي والتي ارتبطت بظهور مجتمع المعلومات العالمي.

والى جانب ما مثل ذلك من استخدام سلمي ذي طابع مدني ظهرت استخدامات غير سلمية أخرى للفضاء الالكتروني باستغلاله كساحة جديدة للصراع الدولي ووجه آخر للنزاعات التقليدية التي تخوضها الدول أو الحركات الراديكالية على خلفيات دينية أو عرقية أو ايدولوجية أو حتى مصلحيه ،وأخذت تلك الصراعات الالكترونية تستخدم كافه السبل في شكل ظاهرة الإرهاب الالكتروني من خلال التزاوج ما بين تكنولوجيا الاتصال والمعلومات والإرهاب والحرب ليعبر ذلك عن إحدى القضايا الدولية المعقدة في العصر الحديث، ليس فقط في الإشكاليات التي تفرضها ولكن أيضا في التكتيكات والاستراتيجيات والتحديات أمام كافة الفاعلين من الدول والجماعات والأفراد.

وأصبح الفضاء الالكتروني عالماً موازيا للواقع المادي بكل تعقيداته وأطرافه ومشاكلة وانعكاس ذلك على البيئة الأمنية الدولية وعلى مجتمع المعلومات العالمي وليحمل ذلك معه ظهور أنماط جديدة من التهديدات غير التقليدية ، والتي كان من أبرزها التغير الحادث في نمط استخدام القوة وتحولها في العلاقات الدولية، وذلك في مقابل القوة الصلبة التقليدية التي كانت محور قواعد واطر القانون الدولي، وأصبحت تستخدم القوة المرنة ذات الطابع الالكتروني التي لا تخضع لأي اطر قانونية واضحة .

وجاء ذلك متواكبا مع إمكانية استخدام تلك القوة الجديدة كأداة من أدوات الصراع الدولي وعبر ميدان جديد للصراع وهو الفضاء الالكتروني وشكل ذلك أحد التحديات التي تواجه دورة

وأهميته القصوى للمجتمع الدولي على كافة الأصعدة السياسية والاقتصادية والاجتماعية ، وعبر ذلك الصراع الجديد عن الواقع التكنولوجي للنظام الدولي وليعيد ذلك الاعتبار لقضية العلاقة بين التكنولوجيا والأمن، حيث جاء الصراع في عصر المعلومات متكيفا مع بيئته التكنولوجية الجديدة ويشهد تغير في طبيعتة وآثارة والفاعلين على الساحة العالمية مع تراجع مفهوم سيادة الدولة، وتهاوي الاعتبارات الجغرافية والجيوبوليتيكية والزمنية.

وأصبح الفضاء الإلكتروني شأنه شأن ظاهرة الفضاء التقليدية التي تتألف من أربعه مكونات رئيسية هي المكان والمسافة والحجم والمسار ويعبر محتواها عن طبيعة وجود هذا المحتوى، ويتميز هذا الفضاء الإلكتروني بغياب الحدود الجغرافية وغياب الحكم القاهر لعنصر الزمن والمكان مع اتساعه دولياً وزيادة حجم الفاعلين من خلاله، ومثل بذلك بيئة استراتيجية وساحة جديدة إما لنقل الصراعات من خلاله أو استخدامه نفسه كوسيلة من وسائل الصراع والذي يعد امتدادا طبيعيا للصراع بشكله المادي. وتأثير ذلك على الطابع السلمي للفضاء الالكتروني، والذي يعبر عن فيضا رقمياً من المعلومات لا يعتمد كليا على البيئة المحسوبة التي توفرها شبكات المعلومات بل تتعامل أيضا بكثافة مع مفرداتة ويتعلق اهمها بالعنصر البشري في ظل بروز البيئة الالكترونية التي يعمل بها.

ويتميز الصراع الالكتروني بأنه صراع فيه تدمير لكن ليس فيه بالضرورة دماء وأشلاء، فيه تجسس وتسلل ثم نسف لكن لا دخان ولا أنقاض ولا غبار، ويتميز أطرافه بعدم الوضوح وتكون تداعياته خطيرة سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة والمتنوعة للنيل من سلامة امن الفضاء الالكتروني ،وتتميز تلك الاسلحة بسهوله الحصول عليها وتعلم كيفية استخدامها وتطويرها مع وجود تنوع في الأدوات والآليات من حاسبات الكترونية إلى هواتف محمولة وغيرها والتي دخلت في مجالات التطبيق في كافة مجالات الحياة .

ويعمل انتشار الفضاء الإلكتروني على سهولة الدخول علية واستخدامه من أي فاعل داخل مجتمع المعلومات العالمي، وبما يساعد على توسيع دائرة الهجوم على الأهداف الحيوية وفي نفس الوقت زيادة عدد المهاجمين، فضلا عن طبيعة تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر ذلك عن حالة صراع ممتد يرتبط توظيفه ما بين دافع أيديولوجي وسياسي واقتصادي وإعلامي.

ويعد الصراع الألكتروني حالة سببها تعارض حقيقي أو متخيل للاحتياجات والقيم والمصالح في بيئة يكون وسيطها الفضاء الإلكتروني حيث يشهد حركة التفاعلات بين مختلف أنواع الصراعات. وينشب الصراع الالكتروني من كل أنواع البيئات الأخرى غير المتصلة بالفضاء الإلكتروني و تؤثر فيه كافة النزاعات بين كافة الفاعلين من دول وأفراد وجماعات، ويأخذ كافة الأشكال ما بين صراع سياسي و قانوني وتجاري أو صناعي وتكنولوجي وغيرها بما يعكس كافة مجالات الحياة.

وما الصراع الالكتروني إلا صراع تحركه دوافع سياسية ويتميز بنمطين نمط عنيف يتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني، وذلك بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية عبر أسلحة أدوات الكترونية عبر الفضاء الالكتروني من قبل احد الفاعلين

داخل مجتمع المعلومات العالمي. وهناك نمط أخر للصراع الالكتروني يتميز بطبيعته المرنة عن طريق الصراع والتنافس حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية.

ومن ناحية أخرى أصبح للفضاء الالكتروني دور في إحداث التحول والتغييرات السياسية والاقتصادية والاجتماعية داخل النظام الدولي بتعزيز الانفتاح السياسي والتحول الديمقراطي وظهور ما يعرف بـ "الديمقراطية الرقمية " وتشجيع التغير داخل النظم السياسية الدولية وتشكيل قضايا الرأي العام العالمي وزيادة عدد المساهمين في تشكيلة على المستوى المحلي والدولي، وأصبح للفضاء الالكتروني دور في تغير طبيعة المؤسسات الدولية الحكومية وغير الحكومية والمجتمع المدني العالمي و دفع معدلات النمو الاقتصادي، وتزايد دور المجتمعات المحلية في السياسة الدولية و التي تأخذ صيغه تجمعات الكترونية وأعداد مشتركين بالملايين على مستوى العالم.

وظهر الدور الايجابي أيضا للفضاء الإلكتروني في العمل على تقليل حدة الصراعات فيما يطلق علية بـ "الدبلوماسية الالكترونية" التي تعنى بنشر مبادرات السلام وتعزيز الحوار والتعاون بين دول العالم والانفتاح العالمي على الثقافات المختلفة، وكذلك عمل الفضاء الإلكتروني على زيادة الوعي العالمي بخسائر الصراعات وأثرها على المجتمع الدولي، وبما يعمل على خلق رأي عام دولي يدافع عن خيار السلام وليس خيار الحرب من خلال الدبلوماسية الافتراضية وتعزيز الدبلوماسية الشعبية والقدرة على التأثير في الرأي العام العالمي.

ودفعت تلك التحديات التي يواجهها الفضاء الالكتروني أن جعلت من قضية أمنة تدخل ضمن استراتيجيات الأمن القومي للدول وخاصة بعد أحداث ١١ سبتمبر ٢٠٠١ وانتشار موجه تكنولوجيا الاتصال والمعلومات عالميا وزيادة الاعتماد الدولي عليها في البنية التحتية الكونية للمعلومات، وجاء ذلك مع ضعف الحماية في مواجهة تلك الأخطار تبعا لخصائصها المتغيرة وفق العامل الإنساني الذي يتعامل معه، وعدم وجود أطر قانونية واضحة تحكم ظاهرة الفضاء الإلكتروني وتنظم حقوق وواجبات الدول تجاهها داخل النظام الدولي، ، وأصبحت عملية تنمية القدرات في مجال الفضاء الإلكتروني من العناصر الأساسية للحرب وأصبحت ركيزة أساسية للاستقرار السياسي على المدى الطويل، وظهر التداخل بين ما هو مدني وما هو عسكري.

وأصبحت القوى والأطراف المتعارضة اقل اعتمادا على تسوية خلافاتها داخل النطاق الطبيعي المادي ولكنهم اتجهوا إلى نقل صراعاتهم إلى الفضاء الإلكتروني ليس فقط بين الدول بل بين أطراف عدة بما يتيحه الفضاء الإلكتروني من أدوات جديدة للصراع وأسلحة غير تقليدية متنوعة ورخيصة وسهلة الاستخدام، ويكشف ذلك في الوقت ذاته عن دور لقوة جديدة ذات طابع لين يمكن أن يطلق عليها "القوة الالكترونية " cyber power والتي أصبحت تستخدم على نطاق واسع وممتد باتساع الفضاء الإلكتروني، وظهر استخدام تلك القوة على نحو غير سلمي تعبيراً عن حالة الصراع بين الفاعلين من الدول أو من غير الدول داخل مجتمع المعلومات العالمي، وبما مثل ذلك انتهاكا للطابع السلمي للفضاء

الالكتروني وشكل جديد من استخدام القوة في العلاقات الدولية، تلك القوة التي انتقلت من طابعها المادي إلى طابع الكتروني و تتحرك ويتم استخدامها وينتج عنها الإضرار بالمصالح الإستراتيجية الدولية.

وانعكس ذلك على مصادر القوة وموازينها وطرق توزيعها، والتي أصبحت تعتمد بدرجة اقل على التمسك بالأرض أو القوة العسكرية أو الموارد الطبيعية، وذلك مع بروز القوة المرنة Soft power مقابل تراجع القوة الصلبةHard power في العلاقات الدولية، وأصبح المبدأ الاستراتيجي للاستحواذ على القوة هو العمل على الحصول على مزايا تنافسية بين الفاعلين في المجال المعلوماتي والتكنولوجي.

وتحولت القوة من قوة تعتمد على قوة النيران إلى قوة المعلومات ثم إلي قوة تعتمد على الذكاء البشري، وأصبح الفضاء الإلكتروني لا يختلف عن المجالات الأخرى كالجو والبر والبحر فيما يتعلق بمبادئ الحرب وخصائص القوة حيث تسري في الفضاء الإلكتروني العقيدة العسكرية ذاتها ومجالا جديدا للاستحواذ على القوة بكافة أنواعها.

وترصد الدراسة إلى أن هجمات الفضاء الإلكتروني هي اقرب لنعتها بالإرهاب عن كونها عمل حربي وذلك على الرغم من أن العمل الحربي قد يكون عبارة عن مجموعه أعمال إرهابية، وتعتمد تلك الهجمات على الضربات الاستباقية والتي يمكن أن يقوم بها أفراد وجماعات ودول، وكذلك تميزها بخصائص تعتمد على عنصر المفاجأة والمباغتة وبث الخوف والترويع وتبادل هجمات الكر والفر، ومن ثم ينطلق الباحث إلى تسمية كل هجمات الفضاء الإلكتروني بالإرهاب في إطار الاستخدام غير السلمي للفضاء الالكتروني، والذي أصبح قضية تهدد الأمن الدولي.

ويرجع ذلك للطابع الدولي للظاهرة وخصائصها التي تتعلق بخمسة أبعاد منها البعد التكنولوجي التي يتعلق بالشبكات وتكنولوجيا المعلومات، والبعد الثاني أنها قضية تنموية لان خدمات تكنولوجيا الاتصال والمعلومات تحتاج إلى الأمان وتعتمد على الشبكات في عملها، والبعد الثالث أنها قضية اقتصادية تتعلق بالإبقاء على حالة الأعمال والمزايا الاقتصادية، والرابع يتعلق بكونها قضية قانونية تتعلق بالتعامل مع الجريمة والإرهاب وأهمية التوصيف القانوني للتهديد لتسهيل عملية معالجتها قانونا، ويتعلق البعد الخامس بعلاقة الإرهاب الالكتروني بالأمن القومي وما يتطلبه من أهمية توافر حماية للبنية التحتية الكونية للمعلومات.

ويشير الباحث الى عملية التطور المستمرة في تكنولوجيا الاتصال والمعلومات وما ينتج عنه من بروز أهمية الفضاء الخارجي من ناحية وزيادة تداخله مع الفضاء الإلكتروني من ناحية أخرى، وبما عمل على زيادة أهمية دور الأقمار الصناعية في الحرب والاتصال أو الإرهاب، و بما يعيد الدفع بقوة لتنافس دولي وعسكرة في الفضاء الخارجي في المستقبل المنظور، ويأتي هذا مع زيادة الدول التي تمتلك قدرات فضائية وكذلك التوجه العالمي للاتصال عبر الأقمار الصناعية والإنترنت اللاسلكية بدلاً من الشبكات والكابلات البحرية التي تعاني من مشكلات الانقطاع.

وتتناول الدراسة الإشكاليات التي تعترض تحديد مفهوم الإرهاب الإلكتروني الذي يتداخل مع مفاهيم أخرى كالجريمة الالكترونية وحرب المعلومات والاحتجاج الالكتروني وما يسمى المقاومة الالكترونية، وكذلك تداخل الدوافع بين ما هو سياسي وما هو إجرامي، فضلا عن الاختلاف العالمي

حـول تحديـد مـشروعية الفعـل الإرهـابي، وأن مـا يجمـع الإرهـاب الالكترونـي والمقاومـة أو الجهـاد الالكتروني أنهما شـكل من أشـكال الحـرب عبر الفضاء الالكتروني ، ولكـن الجهـاد الالكترونـي يتميز بأنه يستند إلى أسس أيديولوجية ودينية لتحقيق أهداف محددة.

ويـرى الباحـث أن هجمـات الفضاء الإلكترونـي تزيـل هـذا الارتبـاك حيـث يتميـز الفعـل بطبيعـة وخصائص واحدة تدفع إلى نعته بالفعل الإرهـابي والتي لا يعد الحكم عليه أخلاقيا بقـدر مـا هـو حكـم تقني وفني يرتبط بخصائص مفهوم الإرهـاب في حالة تطبيقهـا علـى كينونـة الفعل وطرق تنفيذه وأثاره، وما يتعلق بمشكلات تحديد ماهية مفاهيم الحرب والسلام والعدوان والهجوم المسلح.

وليخـرج الباحـث مـن هـذا الجدل لصياغة تعريف لمـا قـد يعنيـه الإرهـاب الإلكترونـي بأنـه " نشاط أو هجوم متعمد ذو دوافع سياسية بغرض التأثير علي القرارات الحكومية أو الـرأي العـام باستخدام الفضاء الإلكتروني كعامل مساعد ووسيط في عملية التنفيذ للعمـل الإرهـابي أو الحربـي، أو مـن خـلال مـا يعـد تـأثيرا معنويـا ونفـسيا مـن خـلال التحـريض علـي بـث الكـراهيـة الدينيـة وحـرب الأفكـار، أو إن يـتم في صورة رقمية من خلال استخدام آليات الأسلحة الالكترونيـة الجديدة في معارك تـدور رحاهـا في الفضاء الإلكتروني والتي قد يقتصر تأثيرها علي بعدها الرقمي أوقد تتعدي لإصابة أهـداف مادية تتعلق بالبنية التحتية الحيوية ".

ويعـني الإرهـاب الإلكترونـي كـذلك "العـدوان أو التخويـف أو التهديـد ماديـاً أو معنويـاً باسـتخدام الوسائل الإلكترونية الـصادرة مـن الـدول أو الجماعـات أو الأفـراد عبر الفضاء الإلكتروني أو إن يكـون هدفا لذلك العدوان بما يؤثر علـى الاستخدام الـسلمي لـه "، و يـأتي الإرهـاب الإلكترونـي أيضا في صـورة القيـام بهجـوم طبيعـي عـن طريـق اسـتخدام الأسـلحة التقليديـة في مهاجمـة كـابلات الاتـصال ونقـاط الإنترنت الرئيسية ومحطات البث، أو عن طريق القيام بهجـوم باسـتخدام الطاقة الكهرومغناطيسية ضد أجهزة الكمبيوتر أو البيانات بداخلها بمـا يـؤثر علـى عملها، أو شـن الهجمات باستخدام أسلحة الفضاء الإلكتروني المتنوعة وسهلة الاستخدام وعظيمة الأثر في الإضرار بمصالح المجتمع الدولي.

ومثل ذلك بيئة إستراتيجية لنمو وبروز أشـكال جديـدة مـن الـصراع داخـل الفضاء الالكترونـي و تتعلـق إما بمحاولـة إحكـام الـسيطرة علـى الفضاء الإلكترونـي أو العمـل علـى توظيفـه للاسـتخدام غير السلمي مـن جانـب العديـد مـن الفـاعلين أو حلبـة للتنـافس الـسياسـي والاقتصادي والعسكري والإعلامـي، و مثـل ذلـك الـصراع في الفـضاء الإلكتروني نموذجـاً آخـر ذا طـابع رقمـي عـن النزاعـات التقليديـة الـتي تخوضـها الدول أو الحركات الراديكالية على خلفيات دينية أو عرقية أو إيديولوجية.

وأصبح لكافة الفاعلين داخل مجتمع المعلومات العالمي القدرة والإمكانية في شـن تلـك الهجمـات بعيـدا عـن دور الـدول بمـا سـاهم في إيجـاد فوضـي في اسـتخدام الفـضاء الإلكترونـي، عـبر شـكل جديـد مـن استخدام القوة عبر الفضاء الإلكتروني، واثر ذلك على طبيعة القوة المسلحة ويـأتي هـذا مـع خطـر انتقـال سـاحة المواجهة في الصراع من الفضاء الواقعي إلى الفضاء الإلكتروني ليصبح هنـاك عـالم آخـر بـديلا لمـا يـدور علـى ارض الواقـع، كوجـود مواقـع انترنـت متصلة بالأهـداف الإستراتيجية والمرافق الحيوية يمكـن

ضربها كما يمكن الدفاع والمقاومة لتظهر حرب جديدة بدون إراقة للدماء و لتمثل سلاحاً جديداً وفاعلين جدد يتميزوا بالتنوع مع انتشار الفضاء الإلكتروني الذي هو أوسع من الإنترنت.

وعلى الرغم من تأكيد الباحث على تنوع الفاعلين في الفضاء الإلكتروني باتساعه وخصائصه من الدول والأفراد والجريمة المنظمة أو من يبحثون عن الشهرة والقرصنة، فانه يقدم نموذجاً للفاعلين من غير الدول مثل استخدام الجماعات الإرهابية للفضاء الالكتروني ويقدم الباحث نموذج للفاعلين من غير الدول وهو " تنظيم القاعدة" وهو الذي استخدمه في التجنيد والحشد والتعبئة والتمويل والتنظيم وجمع المعلومات والتنسيق وإضفاء الطابع الدولي على نشاطة والتأثير في الرأي العام العالمي، ونجاحه في نقل ساحة المواجهة مع الولايات المتحدة من الفضاء الواقعي للفضاء الإلكتروني. ويلاحظ الباحث أن استخدام تنظيم القاعدة للفضاء الالكتروني غلب عليه استخدامه كوسيلة إعلام دولية الطابع في مقابل ضعف اهتمامه بتطوير أسلحة أو استخدام هجمات الفضاء الالكتروني ولكن هذا الاهتمام قد يتصاعد في المستقبل.

ويرى الباحث انه على الرغم من سعى الجماعات الإسلامية إلى أن تصبح قوة إلكترونية هامة قادرة على إنزال الأضرار الجسيمة وأكثر بكثير من تلك التي قد يسببها هجوم إرهابي تقليدي إلا إن هناك فجوة كبيرة بين طموحات تلك الجماعات وبين قدراتهم الفعلية على تحقيق هذه الطموحات. ورغم أنهم يدعون نيتهم ورغبتهم في مهاجمة أهداف اقتصادية هامة، وأنظمة حكومية على الشبكة الالكترونية ومواقع حساسة أخرى، بهدف تقويض الاقتصاد الغربي بشكل كامل، إلا أن شبكات المواقع الإسلامية لم تقدم أية أدلة إلى الآن على أن هجمات من هذا النوع قد تم تنفيذها. في حين يظهر لنا أن معظم المواقع التي هاجمها الإسلاميون كانت مواقع فاسدة أخلاقياً أو معادية للإسلام. إضافة إلى ذلك فإن معظم الهجمات التي تم تنفيذها استخدمت فيها طرقاً وأساليب غير متطورة، مما يعني أن هذه الطرق لا تشكل خطرا فعليا وهاماً على المصالح الاقتصادية الغربية، أو البنية التحتية الحساسة لهذه الأنظمة على الأقل في هذه الفترة لا يزال يشكل إزعاجاً أكثر منه تهديداً فعلياً.

ومن المتوقع ان يزداد قوة في المستقبل خاصة مع قدرة المهاجمين على الدخول إلى شبكات الأنظمة الأمنية الحساسة. وازدياد التواصل وتبادل الخبرات بينهم سيضيق من الفجوة بين أهداف هذه المجموعات وقدراتها الفعلية على تنفيذ أهدافها بالإضافة إلى تحول الجماعات الإرهابية من العمل الفردي إلى العمل الجماعي المنظم عبر الفضاء الالكتروني مع انتشار الدخول للفضاء الالكتروني عالميا وبما يشكل زيادة في خطورة تعرض الشبكات الالكترونية والبنية التحتية الكونية للمعلومات للخطر .

و يقدم الباحث نموذجاً لحالة استخدام الفاعلين من الدول للفضاء الإلكتروني في تطوير أسلحة الكترونية بل وسعى الدول إلى تطوير ترسانة أسلحة الكترونية وتخصيص ميزانيات لتطويرها ،بالإضافة إلى استخدام الفضاء الالكتروني في عمل أجهزة الاستخبارات الدولية و دوره المؤثر على عملها بتوفير بيئة جديدة لها وفاعلين جدداً وادوات جديدة، وبما شكل ميزة إستراتيجية في تجنيد العملاء أو سرقة الأسرار، وشن الحرب النفسية من خلال نشر معلومات وبيانات مضللة أو التحريض

على الكراهية الدينية أو التأثير على الرأي العام من اجل دفعه لموقف معين سواء من خلال المنتديات الحوارية وبرامج الدردشة.

وقد يقف جهاز استخبارات خلف موقع يبدو انه معاد، ولكنها تستغله لجذب المتعاطفين معه وجمع معلومات عنهم وفهم أفكارهم والدعاية والترويج لسياسة الدولة عن طريق مواقع الإنترنت التي تتبناها أجهزة الاستخبارات بشكل مباشر أو وقوفها بشكل خفي خلف مواقع أخرى وغالبا ما تكون مواقع خدمية كتلك التي تقدم خدمات بريدية أو دردشة عبر الإنترنت أو خدمة تنزيل البرامج المجانية، و المساعدة في جمع المعلومات والتنقيب عنها الخاصة بالدول أو الجماعات المعارضة لها سواء في الداخل أو الخارج للمساعدة في خلق رؤية واتجاه عام لديها بخصوصها والتعامل معها، و الاستفادة من الإنترنت والاتصالات في خلق شبكة عملاء دوليين خارج حدود الدولة والمساهمة في إمدادها بشبكة معلومات عن الدولة التي يقيمون بها، و تجنيدهم عن طريق مباشر بالإعلان عن حاجتها لمثل تلك الشبكات.

وقد تستخدم الدول الإرهاب الالكتروني كأداة في الصراع مع غيرها من الدول أو ضد فاعلين من غير الدول أو قد تستخدمه لدعم جماعات ضد جماعات أخرى داخل الدولة أو بين جماعات عبر الحدود، وقد تمارس الدولة الإرهاب الالكتروني على مواطنيها كحجب مواقع الانترنت أو انتهاك الخصوصية وحرية الرأي والتعبير، بالإضافة إلى استخدام الفضاء الالكتروني كأداة للرقابة والتجسس على الدول والأفراد والجماعات وتطوير أساليب جمع المعلومات، ويؤكد الباحث على أن ذلك الصراع يتميز بأهمية الطابع الفردي والمهارة الشخصية في استخدام الفضاء الإلكتروني للتنافس السياسي والاقتصادي والتجاري والعسكري والعلمي.

ويقسم الباحث أنماط الصراع داخل الفضاء الإلكتروني إلى نمطين: الأول، نمط الحرب البادرة بمعنى الصراعات منخفضة الشدة التي تعبر عن صراعات اجتماعية ممتدة على أسس عرقية ودينية كالصراع العربي الإسرائيلي والصراع ما بين الهند وباكستان حول كشمير أو في حالة الخلاف بين روسيا واستونيا في مايو عام ٢٠٠٧، بالإضافة إلى صراعات ذات طابع تجاري وعلمي للحصول على السيادة والنفوذ، ويتميز هذا النوع من الصراع بأنه لا يتطور بالضرورة لمواجهه عسكرية تقليدية، ومثال ذلك حالة الصراع ما بين الصين والولايات المتحدة أو ما بين روسيا والغرب

وأما النمط الأخر من الصراع الالكتروني فيرتبط بنمط الحرب الساخنة أو الصراعات عالية الشدة والتي يكون فيها الصراع تعبيرا عن حالة الصراع الآنية التي تكون ممتزجة باستخدام القوة التقليدية يتم في شكل سلوك عنيف بشن هجمات الكترونية ضد مواقع دولة معينة أو قصف مادي مباشر للكابلات وخطوط الاتصال أو استخدام القنابل الالكترونية التي تشل عمل الأجهزة، كما حدث في الحرب ما بين يوغوسلافيا وحلف الناتو في ١٩٩٩، وفي الحرب الأمريكية على العراق في مارس ٢٠٠٣، وفي الحرب بين حزب الله وإسرائيل في يونيو ٢٠٠٦. و كحالة الحرب الجورجية الروسية في أغسطس ٢٠٠٨.

وأصبح الفضاء الإلكتروني وسيطا للأعمال العدائية وعنصراً من عناصر القوة، يتم استخدامها في حالات الدفاع أو الهجوم من قبل كافة الفاعلين داخل مجتمع المعلومات العالمي وتتسع عمليات هجمات

الإرهـاب الإلكتروني وتتمـدد ميدانيا لتطال كافـة الفاعلين، ويتم تجـاوز الحـدود الفاصلـة بين مـا هـو مـدني ومـا هـو عسكري ومـا بـين حالـة الحـرب وحالـة السـلام، وبمـا يجعـل صـراع الفضاء الإلكتروني وحـرب المعلومـات الأقـل عنفـا ودمويـة عـن الحـروب التقليديـة والـتي ستشـكل أنمـاط حـروب المستقبل واحداث ثورة في الشئون العسكرية .

كمـا إن تلك الهجمـات أو الصراع لا يوجـد لـه جبهـة قتـال محـددة بـل تتسـع جبهتـه باتسـاع الفضـاء الإلكتروني. وإن الخطر غير الملموس لهجمـات الفضاء الإلكتروني تحـدث ضـرراً اشـد مـن الهجمـات ذات الطابع المادي في الحروب التقليدية معلومة الملامح، في مقابل أن تدمير البنية التحتية للمعلومات ينتج عنه آثار غير ملموسة أو مرئية يصعب التعامل معها مما يجعلها اقرب للعقوبات الاقتصادية في وقت السلم.

وفرض ذلك إشكاليات قانونية حيث إن القانون الـدولي قـد تعامـل مـع حظـر اسـتخدام القـوة الصلبة التقليديـة أو التهديـد بهـا في حـين أن تلـك القـوة الجديـدة "الالكترونيـة " لا يوجـد تكييـف قـانوني واضـح لاستخدامها أو فرض قيود عليها أو تحدد ما هو استخدام مشروع أو غير مشروع لهذا النمط الجديد من القوة، ومن ثم ظهـرت فجوة تشريعية مـا بـين الأطـر القانونيـة الدوليـة الحاليـة والموقـف مـن اسـتخدام هـذا النمط من القوة، إلى جانب إشكاليات تتعلق بطبيعة الهجوم الالكتروني.

ويرجـع ذلـك إلى أن التطـورات التكنولوجيـة أدت إلى تحـدي التغيير في قـدرة الأطـر القانونيـة الدوليـة الحاليـة علـى التعامـل مـع الظـواهر الـتي فرضـتها ظـاهرة الإرهـاب الالكـتروني حيـث فاقـت في تطورهـا القـدرة علـى صياغة إطـار قـانوني للتعامـل معهـا ، وبمـا شـكل تحـديا جديـا للقـانون الـدولي، حيـث غابـت أطـر قانونيـة واضـحة للتعامـل مـع اسـتخدام القـوة في الفضـاء الإلكـتروني أو تحديـد اسـتخداماته السـلمية وغير السلمية وعلاقة ذلك بمبـدأ حظـر اسـتخدام القـوة في العلاقـات الدوليـة الـوارد في المـادة ٢ فقـرة ٤ مـن ميثاق الأمم المتحدة ، ومدى إمكانية أن يتم تطبيـق ذلـك علـى هجمـات الإرهـاب الالكـتروني. وبمـا تطلـب ضرورة التعامـل وصياغة الأطـر القانونيـة الـتي تحكـم اسـتخدام الفضـاء الإلكـتروني شـأنه في ذلـك شـأن غيره مـن المجـالات الـتي يمـارس فيهـا الإنسـان نشـاطه كـالبر والبحـر والجـو والفضـاء الخـارجي بحيـث تحكمه القواعد العامة التي تحقق صالح المجتمع الدولي.

ويفـرض ذلـك أهميـة مواءمـة الفضـاء الالكـتروني بتقـدم قـانوني أخـر يواكبـه ويحـافظ عليـه ويكفـل حمايته ويضع الحلول لما يطرأ عليه من مشكلات بسبب استخدامه حتى يصبح أداة للبنـاء وأساسـا لكـل تطور، وأن دور القانون لا يقف عند مجرد تنظيم العلاقـات المترتبـة علـي اسـتخدام الفضـاء الالكترونـي بـل يجب أن يمتد ليحمي القيم التي تحيط باستخدامه ويحدد المسار الصحيح الـذي يجـب إن يسـلكه حتـى لا يتخذه الإرهابيون على اختلاف درجاتهم وشخوصهم أداة لتطوير وسائلهم.

ويتطلب هـذا أن يمتـد القـانون مـن خـلال نصوصـه إلى تلـك الأنشطة الجديـدة ذات الطـابع غـير السـلمي للفضاء الالكتروني من خلال تحديد الوضـع القـانوني بشـأن تلـك الظـاهرة، خاصـة أنـة لم يـتم الإشـارة في إي مـن النصـوص القانونيـة الدوليـة الحاليـة إلى مسـألة اسـتخدام الفضـاء الالكترونـي كـأداة مـن أدوات الـصراع المسـلح، ومـا يمكـن أن يكـون لهـذا الاسـتخدام مـن تـداعيات علـى البنيـة التحتيـة الكونيـة للمعلومات تتسم بالجسامة والخطورة على المجتمع الدولي قاطبة.

ويشير الباحث انه إذا كانت تلك الأطر القانونية الدولية التي استقرت على مخاطبة الدولة باعتبارها فاعلا هاما في العلاقات الدولية فان تلك القواعد يجب أن تنسحب أيضا على الفاعلين من غير الدول باعتبارهم أيضا فاعلين داخل مجتمع المعلومات العالمي، و إن الطابع العالمي للفضاء الالكتروني يجعل من الإرهاب الإلكتروني كقضية دولية وعالمية ومن ثم فان من يتحمل المسئولية ليست فقط الدول، ويعزز الطابع الدولي للقضية أهمية المنظمات ذات الطابع والنشاط الدولي وأهمية بث ثقافة مشتركة عالمية تحافظ على ارث الحضارة الإنسانية ولكون ذلك الخطر عالمي الطابع والملمح فانه يتطلب تعاونا دوليا كذلك.

ويؤكد الباحث أن غياب اتفاقية واضحة على المستوى الدولي للتعامل مع ظاهرة الفضاء الإلكتروني وتنظيم استخدامها وتوضيح الحقوق والواجبات قد يجعل الدول لا تشعر بأي إلزام تجاه التعاون مع غيرها، ومن ثم فان عدم التعاون يشكل جزءا هاماً من تعقد المشكلة وبما يؤثر على معرفة الهجوم ومواجهته، حيث أن هدف التعاون هو "حماية السيادة والأمن والمصالح الأساسية المشتركة"، فتعرض الدول لهجمات الشبكات وقواعد البيانات يمثل جزءا من مصالحها الوطنية وفي تطورها التكنولوجي وفي مساعيها لحماية أمنها وخصوصية مواطنيها، وتمثل القواعد القانونية ضغطا دبلوماسيا على تلك الدول التي لا تعترف أو تدرك بان هجوم الإرهاب الإلكتروني يعد جريمة دولية، وهذا الضغط الدبلوماسي سيمهد الطريق لتعزيز الرؤى حول خطورة استخدام تلك الهجمات كأداة من أدوات الصراع، وسيحتم ذلك تعاونا جادا بين دول العالم.

ويتم النظر إلى الدول التي تتقاعس عن التعاون على أنها لا تساهم في دعم الأمن الدولي ومن ثم تشكل خطرا علية، أو أنها تقع في موقف الاتهام بالعمل على زعزعة الأمن والاستقرار الدولي أو بتجنيد من يقفون خلف هجمات الإرهاب الإلكتروني عن طريق تجنيد أفراد للقيام بهجمات بالنيابة عنها، وهذا ما يعد عملا من أعمال الحرب وإضرارا بالغا بالطابع المدني والسلمي للفضاء الالكتروني، كما أن وجود اطر قانونية دولية تتعامل مع تلك الظاهرة من شأنه أن يدعم الأطر الوطنية داخل كل دولة على حدة وعلى المستوى الدولي ككل.

ويجتهد الباحث في وضع حل لتلك المشكلة في الاستناد إلى العرف والقياس كأحد مصادر القانون الدولي من خلال تعرض الباحث إلى تلك الهجمات وخصائصها ومدى تعارض عملية استخدامها مع مبادئ قانون الحرب التي تنظم حالة استخدام القوة في الصراع المسلح سواء في حالة النزاع المسلح أو في حالة الدفاع الشرعي.

وأن هناك ضرورة في أن يركز المجتمع الدولي في معالجته لظاهرة الإرهاب الالكتروني على نتائجها بالإضافة إلى الناحية العملياتية آو الآلية التي تتم بها والتي يتم من خلالها عملية التأثير وذلك بدلا من التركيز بصورة اكبر على إثارة الجدل حول توصيف الفعل داخل الفضاء الالكتروني حيث من الأفضل ان يتم رؤية أي نشاط وتصنيفه على انه سلمي أو غير سلمي.

وللوقوف حول مدى مشروعية استخدام هجمات الإرهاب الالكتروني كاستخدام للقوة في العلاقات الدولية وعلاقة ذلك بمبدأ حظر استخدام القوة الوارد في المادة ٢ فقرة ٤ من ميثاق الأمم المتحدة،

فيحاول الباحث الاستفادة الممكنة من الأطر القانونية الحالية وإمكانية تكيفيها معها وكذلك المصادر الأخرى الاحتياطية للقانون الدولي كالعرف والقياس، ومن هذا المنطلق يقوم الباحث بعقد مناظرة قانونية ما بين مبادئ قانون الحرب أو القانون الدولي الإنساني وما بين خصائص استخدام أسلحة الفضاء الإلكتروني، وكذلك الاستفادة من بعض الأطر القانونية في مبادئها العامة كالقانون الدولي لحقوق الإنسان، وكذلك القانون الدولي للبحار والقانون الدولي للفضاء الخارجي والأجرام السماوية بما أرساه من قواعد وأسس ترسخ فكرة الحفاظ على حقوق الإنسان وتعزيز الأمن الجماعي والإنساني المشترك وكذلك ترسيخ فكرة التراث المشترك للإنسانية. وكذلك استنار الباحث بموقف محكمة العدل الدولية من تجريم استخدام الأسلحة النووية حتى في حالة الدفاع الشرعي .

وبعد دراسة لتلك المواقف والمواثيق الدولية انتهى الباحث إلى نتائج والتي ارتكزت على أسس عملية ونظرية مفادها إن عدم وجود اطر قانونية واضحة تتناول الموقف من استخدام هجمات الإرهاب الإلكتروني لا يشكل مبررا لاستخدامها حيث أنها تتناقض بل وتتعارض تعارضا بينا مع الأطر العامة للقانون الدولي ومبادئ القانون الدولي الإنساني، ومن ثم فان استخدامها أو التهديد بها يعد غير قانوني ويمكن أن يرتب عليه المسئولية القانونية ، كما أنها تمثل تهديدا للأمن الجماعي الدولي وتهديدا للبنية التحتية الكونية للمعلومات بتعرض الفضاء الإلكتروني للخطر لما يمثلة من أهمية إستراتيجية للمجتمع الدولي.

وهناك صعوبة في تحديد أشكال الإرهاب والحرب داخل الفضاء الإلكتروني وإمكانية اعتبارها نوعا من ممارسة "القوة أو الحرب أو العدوان وفق المنطوق التقليدي للقانون الدولي فان ذلك لا يعني أولا : أن الأطر القانونية الدولية لم تحمل حتى في أطرها العامة ومقاصدها حماية ضد تلك الهجمات، وثانيا :إن الاختلاف في توصيف تلك الهجمات مع تنوعها لا يجب أن تمنع المجتمع الدولي من للتركيز على أضرارها وتداعياتها فيما يتعلق بالطابع السلمي للفضاء الالكتروني ككل، وما يتعلق بذلك من تعرض المصالح الدولية للخطر.

وخاصة أن الفصل السابع من الميثاق أعطى الصلاحية لمجلس الأمن بشأن ما قد يرتئيه مهددا للسلم والأمن الدوليين وحشد الجهود الدولية في مواجهه العدوان، فحتى إذا ما تم اعتبار كثير من هجمات الإرهاب الالكتروني جزءاً من "استخدام القوه " أو "العدوان " فانه يمكن اعتبارها بكل تأكيد أخطاراً تهدد السلم الدولي وحتى إذا كانت مقتصرة فقط على تهديد الحكومات الوطنية فإنها تعد كذلك مهددا للسلم الدولي.

ومن ثم فان هجمات الإرهاب الالكتروني هي نوع من أنواع ممارسة القوة في العلاقات الدولية حيث يمكن استخدام تلك الهجمات لمهاجمة مراكز التحكم والسيطرة للهجوم على شبكات الطاقة وعلى أنظمة التسلح، حيث ينتج عن تلك الهجمات تدمير مادي ونتائج وآثار تدميرية توازي ما ينتج عن استخدام الأسلحة التقليدية وغير التقليدية ، وذلك عن طريق توظيف هجمات شبكات الكمبيوتر في المستويات العملياتية أو الإستراتيجية وان ما يترتب عن هجمات الفضاء الإلكتروني من أثار مادية ونفسية لا حدود

لها وما تمثله من خطورة لعمل البنية التحتية الكونية للمعلومات،وبما يجعل البشرية هي محل الاعتداء نظرا للطابع الدولي للفضاء الالكتروني.

وقد تستخدم هجمات الإرهاب الالكتروني في شكل عمليات للدفاع او الهجوم ، وان كان الدفاع قد يكون شرعيا ويمثل مقاومة ودفاع شرعي عن النفس فان الهجوم قد يحمل أيضا مدلولات العدوان حيث يتم استخدامها وفق مشروعيه الموقف أو الدافع ورائها وقد تشن الدول هجمات الفضاء الالكتروني كجزء مما تعتبره دفاع شرعي عن النفس الذي يبيحه القانون الدولي ويأتي هذا مع بروز ظاهرة المقاومة الالكترونية التي تقوم بها الجماعات من غير الدول في إطار الدفاع عن العدوان .

وتتعلق آليات وإستراتيجيات استخدام الفضاء الالكتروني في المقاومة الالكترونية عبر نمطين يتعلق الأول بالاستخدام والتوظيف الإعلامي للفضاء الالكتروني كوسيلة أعلام دولية الطابع عن طريق استخدام كافة أدوات الرأي والتعبير عبر الانترنت للتعبير عن وجهات النظر والتأييد ، وجمع التوقيعات الالكترونية واستطلاعات الرأي الالكترونية التي تبرز مواقف المشاركين من طرفي النزاع، وغرف الدردشة والمنتديات في الإنترنت للقيام بحوارات وتكوين رأي مناصر؛ وتكوين التحالفات السياسية ونشر أفكار المظاهرات والاحتجاج وإنشاء مواقع انترنت لنشر الأفكار والرؤى الخاصة بالموقف الاحتجاجي للحصول على تأييد الرأي العام وتجنيد الموالين والداعمين.

أما عن النمط الثاني فيتعلق برد الفعل العنيف عن طريق التحول من لغة الحوار والإقناع إلى التدمير والإقصاء عبر القرصنة والاختراق لشل وتعطيل وتدمير الموقع ووقفه عن العمل وإغراقه بآلاف الرسائل الالكترونية ، وقد يحمل بعضها فيروسات تؤدي لعرقلة عمل الموقع واختراقه وسرقة المعلومات ونشر الفيروسات، و إرسال كم كبير من الرسائل الاحتجاجية لكافه الأطراف المعنية بصورة ضاغطة ومزعجة عن طريق البريد الإلكتروني.

ومن منطلق أن عمليه استخدام هجمات الإرهاب الالكتروني تتعارض مع مبادئ وقواعد القانون الذي يتناول النزاع المسلح، وبالنظر إلى الاعتبارات الإنسانية التي تخضع الأعمال المسلحة لعدد من المطالب والشروط لذلك فان وسائل وطرق الحرب التي ربما تعمل على إزالة التمييز ما بين الأهداف المدنية والعسكرية التي قد يترتب عن استخدامها آلام أو أضرار لا مبرر لها للمحاربين تصبح محرماً استخدامها ، وبالنظر كذلك إلى خصائص أسلحة الفضاء الإلكتروني التي تجعل من نتائج استخدامها كارثية بما يجعلها تخضع للاعتبارات القانونية التي يتم التعامل بها وخاصة قواعد النسبية والضرورة والوسطية والتمييز والحياد والإنسانية والمدنيين والمنشآت المدنية.

ومن ثم فان استخدام تلك الأسلحة عبر الفضاء الالكتروني في حالة النزاع المسلح تمثل انتهاكا لمبادئ القانون الدولي. وحتى أنه إذا لم يتم اعتبار هجمات الفضاء الإلكتروني و حرب المعلومات لا تعد شكلا من أشكال الحرب فانه حينئذ لا يسري القانون الدولي الإنساني عليها فان تلك الهجمات يمكن اعتبارها والنظر إليها كإجراءات غير مباشرة للحرب أو نوعا من الأعمال العدائية غير العسكرية من قبيل غلق الممرات المائية أو فرض العقوبات التجارية والاقتصادية ومن ثم فان التصرف الذي يمكن أن تقوم به الدولة يمكن النظر إليه على انه يمثل حقاً شرعياً لها.

أما مشروعية استخدام تلك الأسلحة في حالة الدفاع الشرعي على الرغم من إمكانية إباحته إلا انه قد ينطوي على مخاطر بانتهاك مبادئ القانون الدولي التي تتعلق بالحفاظ على السلم والأمن الدولي والحفاظ على حيادية الفضاء الالكتروني كوسيلة إعلام دولية وكمرفق دولي يحمل أهمية إستراتيجية للمجتمع الدولي ومن ثم فان كان هناك اتجاها لمشروعية استخدامه في الدفاع الشرعي فانه يجب العمل على عدم اتساع ذلك الحق لأنة قد يجلب من الأضرار أكثر مما يجني من فوائد وخاصة الأضرار بقيمة حرية الرأي والتعبير وقيمة الأمن .

و بالنظر إلى الجهود الدولية للحد من انتشار الأسلحة التقليدية وأسلحة الدمار الشامل فانه يمكن النظر إلى هجمات الإرهاب الإلكتروني باعتبارها تقع تحت مسمي " الوسائل الالكترونية للتدمير الشامل " .(EMMD) "Electronic Means of Mass Disruption ، و تكون تداعيات هجمات الإرهاب الالكتروني عشوائية وبعيدة الأثر التدميري وبشكل يجعلها تقترب من توصيف أسلحة الدمار الشامل والتي تفتقد القدرة على التمييز وعلى محدودية إصابة الهدف حيث تتسبب في أضرار بالغة وكارثية على الجانب المدني والعسكري، ومن ثم فان أسلحة الفضاء الإلكتروني لا تمتلك القدرة على التمييز كما أنها عابرة للحدود وذات علاقة بالبنية التحتية الكونية للمعلومات بما يتسبب في الإضرار بالمدنيين أو البيئة أو المنشآت التي تحتوي على خطورة خاصة ويفرض ذلك الحاجة للاتفاق حول قانون دولي جديد يتعامل مع الوسائل الالكترونية للتدمير الشامل (EMMD).

ويستند الباحث إلى موقف محكمة العدل الدولية من استخدام الأسلحة النووية في حالة الصراع المسلح والمتعلق بتجريم استخدامها حتى في حالة الدفاع الشرعي في عملية تطوير موقف قانوني من هجمات الفضاء الإرهاب الالكتروني ولينتقل الباحث إلى اعتبار أن نتائج هجمات الإرهاب الالكتروني يمكن أن يتم التعامل معها وفق المحكمة الجنائية الدولية على اعتبار أنها تمثل شكل من أشكال العدوان بالاستناد على تعريف الجمعية العامة للأمم المتحدة له وبما قد يدخلها ضمن ثلاثة أنواع من الجرائم ضد الإنسانية وجرائم الإبادة الجماعية وجرائم الحرب وخاصة مع صعوبة تطبيق اتفاقيات الحد من التسلح على الأسلحة الالكترونية حيث ضعف القدرة على مراقبة نقل أو تطوير أو استخدام أو تخزين الأسلحة الالكترونية.

أما عن موقف الشريعة الإسلامية من استخدام الإرهاب الالكتروني فان هناك جانب من الفقهاء يجمعوا على تحريم العدوان وان استخدام تلك الهجمات قد يكون مشروعا في حالة التعرض للعدوان أو الدفاع الشرعي، أما الباحث فيميل إلى الاتجاه الأخر الذي يرى أن الإسلام قد سبق القانون الدولي الإنساني في وضع قواعد للحرب والقتال بغية عدم الأضرار أو إفساد في الأرض والتأكيد على التمييز بين المحاربين وغير المحاربين ومن هذا المنطلق فإن انتفاء هذا التمييز تصبح معه عملية شن هجمات الإرهاب الالكتروني غير مشروعه تبعاً لخصائصها المعروفة .

وتبقى مسألة التعاون الدولي هامة حيث أن الأخطار الالكترونية ذات طبيعة عالمية وتحتاج بالتالي إلى حل عالمي، وهذه التحديات تحتاج إلى الكفاية والتدابير القانونية والتقنية المتخذة، وعلى الرغم من عدم وجود اتفاق دولي ينظم التعامل مع الفضاء الإلكتروني إلا إن هناك وعياً متزايداً داخل بلدان العالم

بشان تلك الأخطار، والتي دفعت بعض البلدان إلى تنبي تشريعات خاصة بالجريمة الالكترونية، و إن الأهمية الإستراتيجية للفضاء الالكتروني للمجتمع الدولي تدفع أولا إلى إن يضطلع بدور في إدارته تحت مظلة الأمم المتحدة أو المنظمات الدولية المتخصصة كالاتحاد الدولي للاتصالات، على اعتبار إن الفضاء الإلكتروني مرفق دولي وتقع به مصالح جميع الدول، وتجاوزه للحدود القومية وللسيادة التقليدية للدول.

ويعمل ذلك على وجود صعوبة تتعلق بقدرة الدولة بمفردها السيطرة عليه أو أن تتحمل بمفردها مسئولية حل مشاكل الأمن الالكتروني، وبما يستلزم ذلك ضرورة إيجاد طرق جديدة للتعاون الإقليمي والدولي، وما يحمل من أثار ايجابية فيما يتعلق بتشجيع أنشطة الحماية الرئيسية وتنمية المستويات الدولية لها والتنسيق بين النظم القضائية في العالم والعمل على مساعدة الدول النامية. ومن شأن ذلك أن يعمل على إحراز تقدم في مجال مكافحة هجمات الفضاء الإلكتروني. وتؤكد الدراسة على أهمية التعاون الدولي في مواجهه الأخطار التي تأتي أو تؤثر في الفضاء الإلكتروني، كما إن الدول التي لديها قابلية اكبر لتعرض لمثل تلك الأخطار أصبحت بحاجة ملحة للتعاون مع الدول التي ليس لديها مثل تلك القابلية حيث إن ذلك الخطر يتميز بطبيعته الشاملة وتأثيره الممتد بين الدول العابر للحدود حيث يتم شن هجمات الفضاء الإلكتروني من أي مكان وفي أي زمان وهذا ما يستلزم وجود ائتلاف دولي لمواجهة هذا الخطر.

ومن ثم فإن أي إجراءات أمنية تتعلق بالحماية من خطر التعرض للإرهاب الالكتروني تتفذها الدول فرادى لا تكون فعالة على نفس الدرجة إذا ما تمت على المستوى الدولي أو الثنائي على الأقل، وتتطلب الحماية تعاونا داخل الدولة بين كافة الهيئات المعنية والقطاع العام والخاص والشركات العاملة في مجال تكنولوجيا الاتصال والمعلومات من اجل وضع إستراتيجية موحدة للأمن الالكتروني، وقد تكون الآليات الرسمية فعالة في بعض الدول إلا أنها قد لا تكون فعالة في أخرى تحت تأثير البيروقراطية كما إن إدراك الأخطار التي تهدد أمن الفضاء الإلكتروني سواء القائمة أو المحتملة من شأنه أن يدفع الدول إلى اتخاذ خطوات هامة في سبيل المواجهة والتي قد تشمل إجراءات قانونية وتقنية أو سياسية، إلا أنها قد لا تكون فعالة في الدول الأخرى في مواجهه الإرهاب الإلكتروني وهذا ما يتطلب أهمية عقد اتفاقيات ثنائية،

وهناك أهمية لنشر الوعي على المستويات المحلية والدولية بشأن الإرهاب الإلكتروني والجريمة الالكترونية وغيرها من الأنشطة التي تعد انتهاكا للاستخدام السلمي للفضاء الالكتروني وكذلك تحمل انتهاكا لمبدأ حظر استخدام القوة في العلاقات الدولية والتي يمكن أن تساعد الأطراف المعنية للعمل مع الدول الأخرى لتعزيز التعاون المشترك، وتحديث الأطر التشريعية لسد الفجوة في التعامل مع الإرهاب الإلكتروني، للحد من تلك الظاهرة والسيطرة على الفوضى داخل الفضاء الإلكتروني وعلى الرغم من إمكانية استثمار ما تم التوصل بشأنه من خلال الأمم المتحدة مثل القوانين المنظمة لحالة الحرب فيما يعرف بقانون الحرب، فان هناك حاجة إلى إنشاء قواعد قانونية جديدة واتفاقيات على المستوى الثنائي والإقليمي والدولي وفي إطار الأمم المتحدة لتحديث القانون الدولي وجعله يلائم

التطورات الجارية على الصعيد الدولي سواء في طبيعة الظواهر الجديدة أو ما يتعلق بدور الفاعلين داخل مجتمع المعلومات العالمي وعبر أحد مظاهره وهو الفضاء الإلكتروني.

ويجب أن تتم مواجهه الإرهاب الإلكتروني عالميا من خلال ثلاثة مستويات أولها المستوي الرقمي الذي يتم عبر انتهاج سياسة تقنية لأمن المعلومات للمنشآت الحيوية والمكافحة الأمنية للمواقع التي تحض علي الإرهاب والكراهية أو التي توفر معلومات مساعدة للعمل الإرهابي، أما الثاني فيتم من خلال العمل علي مكافحة الإرهاب المادي فلكي يتم نجاح المكافحة علي الفضاء الإلكتروني لن يكون منفصلا عن مواجهته علي ارض الواقع ، والعمل على تأمين كافة المنشآت الحيوية أمنيا وتدريب المسئولين عن مكافحة الإرهاب علي التعامل مع السياسات الأمنية الإلكترونية ، ويأتي الثالث وهو الأهم علي اعتبار أن الفكرة هي التي تحرك القوة ومن ثم فتتم المواجهة اللينة مع الإرهاب من خلال دحض أفكاره وعزله عن المجتمع ببث أفكار مضادة لما يروج له الإرهابيون وإتاحة الفرصة لحرية التعبير حتى يتم عزل تلك الأفكار المتطرفة ومنعها من تضخيم حجمها وحجم المؤيدين لها والحد من استخدام الفضاء الالكتروني في بث الكراهية الدينية وازدراء الأديان.

وتتوقف فاعلية مستويات المواجهة تلك علي حيادية الأداة أو الآلية المنوطة بها المكافحة وذلك بعيدا عن محاولات تسييسها سواء أكانت في إطارها داخل الدولة أو علي المستوي الأهم وهو المستوي الدولي من خلال العمل في إطار الأمم المتحدة علي إيجاد جهة دولية محايدة ذات طابع استقلالي تمارس هذا الدور، ويؤكد الباحث أن ذلك يفرض على ميثاق الأمم المتحدة، وأيضا تحدي إعادة تعريف مفهوم القوة والهجوم المسلح والعدوان ليتواكب مع استخدام الإرهاب الإلكتروني بما يساعد على التكيف القانوني له، وبما يؤثر بالتالي على طرق المواجهة والتعاون الدولي، وأهمية دور الأمم المتحدة في عقد اتفاقيات لحماية البنية التحتية الحرجة لأنظمة المعلومات بوضعها خارج إطار الهجمات أو وضعها تحت وصايتها خلال الأزمات، و يمكن أن يتم وضع الإرهاب الإلكتروني وحرب المعلومات ضمن اتفاقيات الحد من التسلح، و العمل على الموازنة بين متطلبات الأمن فيما يتعلق بعمليات الدفاع وعمليات الهجوم في مواجهة الإرهاب الإلكتروني.

وتتطلب زيادة الوعي بخطر التعرض لهجمات الإرهاب الإلكتروني والجريمة الالكترونية تنمية الوعي لدى المستويات المحلية والدولية حتى يتم تبني إستراتيجية أمنية دولية داخل المجتمع الدولي بما يكفل أهمية التعاون بين الحكومات والشركات من القطاع العام والخاص وحتى من الأفراد في مجال المكافحة وذلك تبعا للبعد الدولي للخطر والطابع الفردي في حدوثه، وأيضا أن تكون هناك صلات ما بين المستويات المحلية والدولية عن طريق الاتفاقيات الثنائية أو الإقليمية أو الدولية، وذلك لكون الإجراءات القانونية تلعب دورا هاما في مواجهه الإرهاب الإلكتروني وذلك تبعا لطبيعة الجريمة متعدية الحدود وخصائصها الجديدة وتشكل في الوقت نفسه أرضية دولية للتعاون في مجال الإجراءات التحقيقية والجنائية بين الدول الأخرى. والعمل على خلق إطار تشريعي وقانوني دولي يتعامل مع الإرهاب الإلكتروني كجريمة سياسية وفي ذات الوقت مواجهة كافة مظاهر الاستخدام الضار وغير القانوني للفضاء الالكتروني كاستخدامه في الجرائم ذات البعد الداخلي أو الدولي.

ويقسم الباحث الجهود الدولية في مكافحة الإرهاب الإلكتروني: إلى عده أنماط النمط الأول يتعلق بالعمل من جانب الدول على إدخال تلك الجرائم ضمن الجرائم الالكترونية والعمل على إصدار تشريعات وطنية تكافح تلك الظاهرة، أما النمط الثاني: سعى عدد من الدول أو التكتلات الإقليمية إلى التعاون فيما بينها في مكافحة الإرهاب والجريمة عبر الانترنت، أما النمط الثالث: فهو العمل على حث الأمم المتحدة على القيام بدور في المكافحة عن طريق فرض سيطرتها على إدارة الانترنت.

ويقر الباحث بأن المجتمع الدولي أصبح بحاجة إلى اكتشاف استراتيجيات واطر للمواجهة تتوافق مع الطبيعة العالمية لهجمات الإرهاب الإلكتروني في شكل مواجهه عالمية. وتبادل الخبرات الأمنية بين الدول من اجل دعم قدرة الدول في الدفاع والحماية ضد الهجمات، والحاجة لتضافر الجهود لأعاده تشكيل نظم سيادة الدول مع ظهور الشبكات الدولية من خلال دعم تجانس القوانين والتعاون في مجال الاستخبارات والحماية ضد تعرض البنَية التحتية الكونية للمعلومات لخطر التهديدات .

وهذا ما يتطلب دورا للأمم المتحدة، وأهمية الموازنة بين حدود الحرية والأمن في استخدام الفضاء الإلكتروني، وذلك إما عن طريق إقامة منظمة دولية خاصة بالأمن الالكتروني أو اتفاقية دولية بشان الفضاء الإلكتروني، أو أن يتم إنشاء منظمة عالمية متخصصة لشئون الفضاء الإلكتروني باستقلال كامل عن هيئة الأمم المتحدة وتتولي وضع القوانين المنظمة لاستخدامه، أو عن طريق العمل على تعزيز دور الأمم المتحدة من خلال منظماتها المتخصصة كاليونسكو أو الاتحاد الدولي للاتصالات وغيرها من سائر الوكالات الدولية المتخصصة التابعة للأمم المتحدة والتي تهتم بشئون الفضاء الإلكتروني كل في حدود اختصاصها وهذا ما يفرض الحاجة إلى نظام قانوني يعمل على تقليص درجات التهديد التي يمثلها استخدام القوة غير المشروع في الفضاء الالكتروني، والعمل على حماية الدول من خطر التعرض لهذا الاستخدام .

ويخلص الباحث إلى التأكيد على أهمية الاستخدام السلمي للفضاء الالكتروني من أجل الحفاظ على تقدم واستقرار المجتمع الدولي الذي أصبح لصيق الصلة به بما يستدعي أهمية إعلان استقلال الفضاء الإلكتروني والعمل على إخلائه من خطر التسلح والعسكرة أو كساحة للصراع الذي وان كان لا تنتهي مظاهره إلا انه يمكن تحجيمه وتطويعه لصالح البشرية جمعاء، على اعتبار أن الفضاء الإلكتروني مرفق دولي وتراث مشترك للإنسانية حيث يجب النظر إليه كوحدة واحدة متكاملة ومجال دولي يحمل خصائص المرفق الدولي.

ويمكن النظر كذلك إلى الفضاء الالكتروني كوسيلة إعلام دولية يجب أن تتمتع بحرية الرأي والتعبير وتلعب دورا في السلام والحوار، مع الأخذ في الاعتبار الموازنة بين مسالة الحفاظ على الأمن في مقابل الحرية التي يجب أن يتمتع بها كحق من حقوق الإنسان، ويستتبع ذلك أهمية وجود ثقافة عالمية لنبذ العنف ومعالجة كافة بذور الصراع والكراهية والفقر والظلم والجهل التي تشكل بيئة دولية لتوالد العنف والإرهاب والحرب بما يوفر بيئة آمنة للاستخدام السلمي للفضاء الالكتروني باعتباره يعزز من أهمية الأمن الجماعي والإنساني المشترك الذي يتعلق في احد عنا صره الجديدة بالأمن الالكتروني الدولي.

وفي سبيل دفع الجهود الدولية لتعزيز دور الفضاء الالكتروني في دعم السلم الدولي من خلال ثقافة عالمية للأمن الالكتروني ومكافحة الاستخدامات غير السلمية وإقامة نظام دولي وقانوني لحمايته يقدم الباحث عدد من التوصيات:

أولاً : بادراك حقيقة أن مواجهه الإرهاب الالكتروني تدفع إلى أهمية التعاون المتعدد بين دول العالم فالقضايا بطبيعتها دولية ومن ثم لكي يتم مواجهتها بفاعلية يتطلب ذلك التنسيق بين كافة مستويات المكافحة المحلية والدولية وبالتعاون مع كافة الفاعلين داخل مجتمع المعلومات العالمي .

ثانيا : تتعلق بضرورة العمل على وضع قواعد دولية تحكم حالات الحرب والنزاع المسلح في الفضاء الإلكتروني وأن يتم فك الغموض والالتباس القانوني وتحديد المفاهيم ذات الصلة التي تتعلق باستخدام القوة في الفضاء الإلكتروني كمفهوم "الهجوم المسلح " ومفهوم "القوة " ومفهوم "العدوان " وإدخال العدوان الالكتروني ضمن أشكال العدوان من اجل دعم الاستخدام السلمي للفضاء الالكتروني

ثالثاً بأن يتم العمل على تحديد القطاعات التي تتعلق بالبنية التحتية الكونية للمعلومات وتحديد مفهومها وأطرها وأهميتها في خدمة الأمن الدولي، ووضع الأمن الالكتروني ضمن استراتيجيات الأمن القومي للدول،

ورابعاً :أن يتم العمل على استقلالية الفضاء الإلكتروني وإخلائه من خطر التسلح أو العسكرة أو ساحة للصراع من أجل تحقيق الأمن والسلام في مجتمع المعلومات العالمي.

خامسا : بالحاجة للقيام بمزيد من التوعية والتثقيف لإعلاء القيم الأخلاقية وخلق ثقافة عالمية للأمن الالكتروني بين كافة الفاعلين داخل مجتمع المعلومات العالمي و تبني إستراتجية دولية مستمرة عبر منظمات الأمم المتحدة المتخصصة كالاتحاد الدولي للاتصالات.

وسادسا: بأن مواجهه الإرهاب الالكتروني لا يجب أن تقتصر فقط على المواجهة الأمنية بل يجب أن تشمل جوانب أخرى تبحث في مسببات عدم الأمن كمعالجة مسببات الصراع والإرهاب والحرب والعمل على توفير بيئة آمنة للاستخدام السلمي للفضاء الإلكتروني.

سابعاً: تتعلق باستنهاض دور الأمم المتحدة للقيام بدورها في تطوير النظام القضائي لهجمات الإرهاب الإلكتروني وتنظيم استخدامه وفق مبدأ حظر استخدام القوة في العلاقات الدولية.

ثامنا : أهمية اعتبار الأمن الالكتروني الجماعي الدولي كأحد أشكال الأمن الجماعي والإنساني الجديد وخاصة مع بروز الفضاء الالكتروني في المستقبل كساحة حرب غير تقليدية

تاسعا: أهمية اعتبار الفضاء الالكتروني وسيلة إعلام دولية الطابع يجب أن يتم استخدامها في تعزيز الأمن والسلم ودعم الحرية، وحقوق الإنسان واحترام التنوع الثقافي والحضاري وأهمية الموازنة ما بين معيار الأمن والحرية.

عاشراً: السعي إلى التوصل لاتفاقية دولية عالمية للأمن الالكتروني وأمن الفضاء الالكتروني و العمل على إنشاء بيئة قانونية تنظر إلى العدوان الالكتروني باعتباره نوعا من أنواع العدوان وإخلالا جسيما بالنظام القانوني الدولي.

# مراجع وهوامش الدراسة

# مراجع وهوامش الدراسة


## أولاً: المراجع باللغة العربية

أ- الوثائق

- ميثاق الأمم المتحدة ٢٦ يونيو ١٩٤٥
- اتفاقيات جنيف الرابعة لعام ١٩٤٩ والبرتوكولات الإضافية لعام ١٩٧٧
- الإعلان العالمي لحقوق الإنسان ١٩٤٨
- اتفاقية القانون الدولي للبحار ١٩٨٢
- اتفاقية الفضاء الخارجي والأجرام السماوية عام ١٩٦٧
- الاتفاقية الأوربية لمكافحة الجريمة السيبرانية ٢٠٠١
- قرارات الجمعية العامة للأمم المتحدة ذات الصلة
- وثائق وقرارات القمة العالمية لمجتمع المعلومات في الدورتين ٢٠٠٣ و٢٠٠٥
- وثيقة مبادرة الاتحاد الدولي للاتصالات للأمن الالكتروني ٢٠٠٧

ب- الكتب

١. إبراهيم عرفات وآخرون، "العولمة والعلوم السياسية "، كلية الاقتصاد والعلوم السياسية، القاهرة، ٢٠٠٠

٢. ابراهيم نافع "انفجار سبتمبر بين العولمة والامركه " مركز الأهرام للترجمة والنشر، القاهرة ٢٠٠٢

٣. احمد ثابت وآخرون، " العولمة وتداعياتها على الوطن العربي "، مركز دراسات الوحدة العربية "، سلسلة كتب المستقبل، يناير ٢٠٠٣.،

٤. احمد أبو الوفا ، النظرية العامة للقانون الدولي الإنساني في القانون الدولي وفي الشريعة الإسلامية ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠٠٦.

٥. ________ ، "القانون الدولي للبحار على ضوء أحكام المحاكم الدولية والوطنية وسلوك الدول واتفاقية ١٩٨٢ "، دار النهضة العربية، القاهرة، ٢٠٠٦

٦. احمد فتحي سرور، " المواجهة القانونية للارهاب "، مركز الاهرام للترجمة والنشر ، الطبعة الاولى ، القاهرة ، ٢٠٠٨

٧. د. أدونيس العكرة "الإرهاب السياسي:بحث في أصول الظاهرة وأبعادها الإنسانية "، دار الطليعة للطباعة والنشر، بيروت، ١٩٨٣

٨. إسماعيل عبد الرحمن "الأسس الأولية للقانون الدولي الإنساني "في القانون الدولي الإنساني دليل للتطبيق على الصعيد الوطني"، دار المستقبل العربي، القاهرة ٢٠٠٣

٩. د. إسماعيل صبري مقلد " أصول العلاقات الدولية إطار عام" الطبعة الأولى، دار النهضة العربية، القاهرة ٢٠٠٧

١٠. انجيليو كودفيلا، المخابرات وفن الحكم " مترجم، محمد صبري الصاوي، الهيئة المصرية العامة للكتاب، القاهرة، الطبعة الأولى، ٢٠٠٦

١١. أمل حمود "مترجم"، روبرت هندي وجوزيف رتبلات، " أوقفوا الحرب.. إزالة النزاع في العصر النووي"، شركة الحوار الثقافي، بيروت، الطبعة: الأولى، ٢٠٠٥

١٢. . امين احمد الحذيفي ، " الحماية الجنائية للاثار " ، دراسة مقارنه ،دار النهضة العربية ، القاهرة ، ٢٠٠٧

١٣. ايثيل دوسو لابول ، "التكنولوجيا والسياسة في عصر المعلومات ،ترجمه ماري عوض ،مراجعه وإشراف زكي الجابر ،ثريا متولي ، المنظمة العربية للتربية والثقافة والعلوم ،تونس، ١٩٨٣

١٤. بن حمودة ليلي ، " الاستخدام السلمي للفضاء الخارجي، "، المؤسسة الجامعية للدراسات والنشر ،الجزائر ، الطبعة الأولى ، ٢٠٠٧

١٥. بولوف، اندرياس فون "المخابرات الأمريكية والحادي عشر من سبتمبر:الإرهاب الدولي ودور أجهزة المخابرات"، ترجمه "عماد بكر"، مكتبة الشروق الدولية، القاهرة، ٢٠٠٤

١٦. تركي ضاهر "الإرهاب العالمي:إرهاب الدول وعمليات الإرهاب "، دار الحسام، بيروت، ١٩٩٤

١٧. تيريزا فرنتس كماتشو(محرر)؛ محمد أمين السلطي، (مترجم)، الأبعاد الدولية لقانون المجال السيبرني، سلسلة اليونسكو، ٢٠٠٢

١٨. حسن الشامي، "وسائل الاتصال وتكنولوجيا العصر "، الهيئة المصريه العامة للكتاب، القاهرة، ١٩٩٧

١٩. د حسن أبو طالب " تحرير وتقديم " تقرير لجنة ٩/١١ تقرير اللجنة الأمريكية القومية عن الهجمات على الولايات المتحدة (مترجم)، مركز الدراسات السياسية والاستراتيجية بالأهرام، مايو ٢٠٠٦

٢٠. حسن عماد مكاوي، "ليلى حسين السيد، " الاتصال ونظرياته المعاصرة " "، الدار المصرية اللبنانية، القاهرة، ١٩٩٨

٢١. د.حسن نافعة، د. سيف عبد الفتاح" إشراف وتحرير"، "العولمة:قضايا ومفاهيم "، كلية الاقتصاد والعلوم السياسية، جامعه القاهرة، ٢٠٠٠

٢٢. د. حسن مظفر الرزو، " الفضاء المعلوماتي" ، مركز دراسات الوحدة العربية ،الطبعة الأولى ، بيروت ٢٠٠٧

٢٣. حشمت قاسم "الاتصال العلمي في البيئة الالكترونية "، دار غريب، القاهرة، ٢٠٠٥

٢٤. عبد العزيز مخيمر عبد الهادي "الإرهاب الدولي مع دراسة الاتفاقيات الدولية والقرارات الصادرة عن المنظمات الدولية " دار النهضة العربية، القاهرة، ١٩٨٦

٢٥. علي محمد رحومة، " علم الاجتماع الآلي، "، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت ٢٠٠٨

٢٦. عبد الناصر حريز، "الإرهاب السياسي دراسة تحليلية"، مكتبة مد بولي، القاهرة، الطبعة الاولى، ١٩٩٦

٢٧. د.محمد بهي الدين عرجون، " الفضاء الخارجي واستخداماته السلمية "، سلسلة عالم المعرفة، عدد ٢١٤، المجلس الوطني للثقافة والفنون والآداب، الكويت، أكتوبر ١٩٩٦، ص ص ١٧٧- ٣٦٧

٢٨. مصطفى عبد الغني، " الرقابة المركزية الامريكيه على الانترنت في الوطن العربي "، دار العين للنشر، القاهرة، ٢٠٠٦

٢٩. د.مصطفي علوي "مفهوم الأمن في مرحلة مابعد الحرب الباردة "، في قضايا الأمن في أسيا "، تحرير (د.هدى متكيس، السيد صدقي عابدين )، مركز الدراسات الأسيوية، كلية الاقتصاد والعلوم السياسية، جامعه القاهرة، ٢٠٠٤

٣٠. مصطفي سلامة حسين، " التأثير المتبادل بين التقدم العلمي والتكنولوجي والقانون الدولي "، دار النهضة العربية، القاهرة، ١٩٩٠

٣١. سامي احمد عابدين، "مبدأ التراث المشترك للإنسانية:دراسة قانونية لأعماق البحار والفضاء الخارجي والقطب الجنوبي "، دار النهضة العربية، ١٩٨٦

٣٢. منير محمد الجنبيهي "امن المعلومات الالكترونية "، دار الفكر الجامعي، القاهرة، ٢٠٠٥

٣٣. د.نبيل احمد حلمي "القانون الدولي وفقا لقواعد القانون الدولي العام، دار النهضة العربية ١٩٩٩

٣٤. نخبة من المتخصصين "القانون الدولي الإنساني:دليل التطبيق على الصعيد الوطني " تقديم، احمد فتحي سرور، دار المستقبل العربي، ٢٠٠٣

٣٥. نخبة من المتخصصين والخبراء "دراسات في القانون الدولي الإنساني "، تقديم د.مفيد شهاب، الطبعة الأولى، دار المستقبل العربي، القاهرة ٢٠٠٠

٣٦. نعوم تشومسكي وآخرون "العولمة والإرهاب:حرب أمريكا على العالم "، د.حمزة المزيني (مترجم )، مكتبة مد بولي ٢٠٠٣

٣٧. نعوم تشوميسكي، "إرهاب القراصنة وإرهاب الاباطره قديما وحديثا"، تعريب احمد عبد الوهاب، مكتبة الشروق الدولية، القاهرة، ٢٠٠٥

٣٨. نعوم تشوميسكي "السيطرة على الإعلام:الإنجازات الهائلة للبروباجندا"، تعريب "اميمة عبد اللطيف، مكتبة الشروق الدولية، القاهرة، ٢٠٠٣

٣٩. نسمه احمد البطريق "الإسلام والمجتمع في عصر العولمة:دراسة في المدخل الاجتماعي"، القاهرة، دار غريب، ٢٠٠٤

٤٠. نزيه نعيم شلالا "الإرهاب الدولي والعدالة الجنائية "، منشورات الحلبي الحقوقية، بيروت ٢٠٠٣

٤١. وائل احمد علام، " الاتفاق التنفيذي لاتفاقية قانون البحار "، دار النهضة العربية، القاهرة، ٢٠٠١

٤٢. هادي خضراوي "ابرز قضايا السياسة الدولية المعاصرة من خلال المفاهيم والبنى "، دار الكتب الحديثة، القاهرة،

٢٠٠٢
٤٣. راسم محمد الجمال "نظام الاتصال والإعلام الدولي:الضبط والسيطرة، الدار المصرية اللبنانية، القاهرة، ٢٠٠٥
٤٤. يحيي اليحياوي، " التكنولوجيا والإعلام والديمقراطية"، دار الطليعة للطباعة والنشر، بيروت، الطبعة الأولى ٢٠٠٤

ج - الدوريات

١. د. الصادق رابح " قراءة في الرهانات الثقافية والاجتماعية للتكنولوجيات الرقمية الحديثة "، مجلة الإذاعات العربية، العدد، ٢٠٠٦.
٢. أسامة دمج: مجلة الإنساني "، اللجنة الدولية للصليب الأحمر الدولي، ربيع ٢٠٠٦
٣. د.بهجت قرني "تراكم الانكشاف الاستراتيجي العربي وأهمية البعد الثقافي المهمل "، مجله المستقبل العربي " مركز دراسات الوحدة العربية، بيروت، مارس ٢٠٠٢، ع ٢٧٧ ص ٥٤- ٦٩
٤. توماس كويلاند (محرر ) " ثورة المعلومات والأمن القومي "، سلسة دراسات عالمية، مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد ٤٦، ٢٠٠٣
٥. جيمس ج. ستيوارت، " نحو تعريف واحد للنزاع المسلح في القانون الدولي الإنساني: رؤية نقدية للنزاع المسلح المدول " المجلة الدولية للصليب الأحمر، ٣١- ١٢- ٢٠٠٣
٦. جون رايان، " حرب المعلومات": تهديد جديد، وسلاح ذو حدّين" الأخطار المتصاعدة: التهديدات الأمنية الناشئة والمتزايدة، مجلة حلف الناتو، العدد الرابع شتاء ٢٠٠٧
٧. جيامباولو دي باولا ، " التحول في رؤيتنا للأمن" ، مجلة حلف الناتو ، العدد الثالث ، خريف ٢٠٠٦
٨. صفات أمين سلامة، "أسلحة حروب المستقبل بين الخيال والواقع "، دراسات استراتيجية، مركز الأمارات لدراسات والبحوث الاستراتيجية، العدد ١١٢، ٢٠٠٥
٩. عادل عبد الصادق " حقيقة دور الانترنت في بث الكراهية الدينية في العالم "ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والإستراتجية بالأهرام، العدد ١٤٤، ديسمبر ٢٠٠٦
١٠. __________ ، " من قطع كابلات الانترنت عن الشرق الأوسط "، ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية، جريدة الأهرام، العدد ١٦٠، ابريل ٢٠٠٨
١١. __________ ، الاحتجاج الالكتروني والفاعلون الجدد في الحياة السياسية "، ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد ١٦٢، يونيه ٢٠٠٨
١٢. __________ ، المدونات كفاعل ونمط جديد في المشاركة السياسية" ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد، ٢٠٠٦
١٣. __________ ، " المدونات من الاحتجاج الشخصي إلى توجيه الرأي العام" مجلة تعليقات مصرية، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد ٦٨، ٢٢ نوفمبر ٢٠٠٦
١٤. __________ ، "الانترنت والإصلاح السياسي في مصر " مجلة تعليقات مصرية، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد، ٨٣، ١٥ يوليو ٢٠٠٧
١٥. __________ ، هل يمثل الإرهاب الالكتروني شكلا جديدا من أشكال الصراع الدولي " ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد ١٥٦- ديسمبر ٢٠٠٧
١٦. __________ ، اختراق مواقع الانترنت بين السنة والشيعة.عندما تسيطر السياسة على الدين"، مجلة تعليقات مصرية، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد ١١٢، ١٥ أكتوبر ٢٠٠٨
١٧. __________ ، قمة تونس العالمية للمعلومات: استمرار الوضع الراهن"، مجلة تعليقات مصرية، مركز الدراسات السياسية والاستراتيجية بالأهرام العدد ٤٤، ٢٢ نوفمبر ٢٠٠٥
١٨. __________ ، " مصر ومجتمع المعلومات: هل يمكن تكرار التجربة الهندية ؟" مجلة تعليقات مصرية، مركز الدراسات السياسية والاستراتيجية بالأهرام العدد ١٧، ١٨ يوليو ٢٠٠٤
١٩. __________ ، العدوان على غزة والمقاومة الالكترونية بين لغه الحواروالتدمير " ملف الاهرام الاستراتيجي، العدد ١٧٠ فبراير ٢٠٠٩

٢٠. د. نبيل علي " عنف المعلومات..وإرهابها " في "مستقبل الثورة الرقمية:العرب والتحدي القادم " نخبة من الكتاب، وزارة الإعلام الكويتية، سلسلة كتاب العربي (٥٥) ١٥ يناير ٢٠٠٤
٢١. نشأت الهلالي "الأمن الجماعي "سلسلة مفاهيم، المركز الدولي للدراسات المستقبلية والاستراتيجية "، العدد ٩، السنة الأولى، سبتمبر ٢٠٠٥
٢٢. مانويل كاستلز "وسائل الاتصال الجماهيرية الفردية الجديدة"، مجلة لوموند ديلوماتيك اغسطس ٢٠٠٦
٢٣. د.محمد بهي الدين عرجون، " الفضاء الخارجي واستخداماته السلمية "، سلسلة عالم المعرفة، عدد ٢١٤، المجلس الوطني للثقافة والفنون والآداب، الكويت، أكتوبر ١٩٩٦،

د. مصادر أخرى

- رسائل علمية منشورة

١. د.حسنين توفيق إبراهيم "ظاهره العنف السياسي في النظم العربية "، أطروحة الدكتوراه، مركز دراسات الوحدة العربية، ١٩٩٢
٢. د.محمد سعدي "مستقبل العلاقات الدولية من صراع الحضارات إلى انسنة الحضارة وثقافة السلام "أطروحة دكتوراه، مركز دراسات الوحدة العربية، بيروت، يونيو ٢٠٠٦
٣. زكريا حسن أبو دامس، " أثر التطور التكنولوجي على الإرهاب"، رسالة ماجستير(منشورة )، قسم العلوم السياسية في الجامعة الأردنية، ٢٠٠٥م، والتي صدرت ككتاب بعنوان " اثر التطور التكنولوجي على الإرهاب "، الطبعة الأولى، ٢٠٠٥ عن دار (عالم الكتب الحديث) ودار (جدار للكتاب العالمي) للنشر والتوزيع بالأردن،
٤. على صادق عبد الحميد صادق، " امن الدولة في النظام القانوني للهواء والفضاء الخارجي "، رسالة دكتوراه، كلية الحقوق جامعه القاهرة، ١٩٧٩

- رسائل علمية غير منشوره

١. احمد جلال الدين عز الدين، " الإرهاب الدولي وانعكاساته على الأمن القومي المصري، رسالة دكتوراه غير منشوره، أكاديمية ناصر العسكرية العليا، كلية الدفاع الوطني، ١٩٨٤
٢. أحمد عبد الونيس شتا ، " الدولة العاصية: دراسة في التعارض بين مواقف الدول والتزاماتها الدولية في الأمم المتحدة مع إشارة خاصة إلى إسرائيل وجنوب افريقيا.- " رسالة دكتوراه، كلية الاقتصاد والعلوم السياسية، القاهرة، ١٩٨٦
٣. إبراهيم زهير الدراجي ،" جريمة العدوان ومدى المسئولية القانونية الدولية عنها "، رسالة دكتوراه ، كلية الحقوق ، جامعه عين شمس ، ٢٠٠٢
٤. أمل محمد فوزي منتصر"، "مجالات استخدام شبكات المعلومات الدولية "الانترنت "في الأنشطة الاتصالية " جامعه القاهرة، كلية الإعلام، رسالة ماجستير غير منشورة، ٢٠٠٤
٥. سعيد حسين محمود غلاب، "التطورات الراهنة في النظام الدولي وإثرها على مبدأ استخدام القوه في العلاقات الدولية " رسالة دكتوراه غير منشورة، كلية الاقتصاد والعلوم السياسية، جامعه القاهرة، ٢٠٠٥
٦. د.عابدين عبد الحميد حسن قنديل، " التدابير المضادة في النظام القانوني الدولي:دراسة نظرية وتطبيقية "، رسالة دكتوراة غير منشورة، كلية الاقتصاد والعلوم السياسية، جامعه القاهرة، ٢٠٠٦
٧. منى محمود مصطفى، "الجوانب القانونية والسياسية لمشاكل الفضاء الخارجي "، رسالة دكتوراة، كلية الاقتصاد والعلوم السياسية، جامعه القاهرة، ١٩٧٥

- ابحاث في ندوات غير منشوره

١. إبراهيم محمد العناني "المحكمة الجنائية الدولية ومنع انتشار أسلحة الدمار الشامل، الفصل الثالث في " اعمل الندوة الفكرية "الخيار النووي في الشرق الأوسط، مركز دراسات المستقبل جامعه أسيوط، ٢٠٠٢.
٢. د.احمد عبد الونيس شتا "القانون الدولي والأسلحة النووية "، بحث غير منشوره ,ندوة "إخلاء منطقة الشرق

الأوسط من أسلحة الدمار الشامل :الجوانب القانونية ،منتدى القانون الدولي ، كلية الاقتصاد والعلوم السياسية ، جامعه القاهرة ، ١٩- ٤- ٢٠٠٤

- جرائد وصحف

١. جريده الأهرام القاهرية
٢. جريدة العالم اليوم، القاهرة
٣. جريدة الشرق الأوسط اللندنية
٤. جريدة الحياة اللندنية
٥. جريدة الخليج الاماراتية
٦. جريد الاخبارالمصرية

- مواقع الانترنت

- موقع مركز الدراسات السياسية والإستراتيجية بالأهرام acpss.ahram.org.eg
- لجنة الصليب الاحمر الدولية http://www.icrc.org/ara
- موقع منظمة الامم المتحدة http://un.org/arabic/law/index.html
- موقع الاتحاد الدولي للاتصالات http://www.itu.int/net/home/index-ar.aspx
- موقع محكمة العدل الدولية /http://www.icj-cij.org/homepage/ar
- منظمة العفو الدولية http://www.amnesty.org/ar
- منظمة الامم المتحدة للعلوم والتربية والثقافة اليونسكو http://typo38.unesco.org/ar/unesco-home.html
- القمة العالمية لمجتمع المعلومات /http://www.un.org/arabic/conferences/wsis
- موقع المبادرة العربية لأنترنت حر /http://www.openarab.net

## ثانيا: المراجع باللغة الإنجليزية

**A- Documents**

- United Nations Charter and related documents 1945
- The United Nations Convention on the Law of the Sea 1982
- Convention on Cybercrime in The member States of the Council of Europe 2001
- Universal Declaration of Human Rights 1948
- International Humanitarian Law - Treaties & Documents

1. Aras P. Suziedelis, **Saving NATO Via a New Trans-Atlantic Bargain: NATO Defense of Cyberspace.** Maxwell AFB, AL, Air Command and Staff College, 2005
2. Arnold K. Veazie, **U.S. Strategy for Cyberspace. Carlisle Barracks**, PA, U.S. Army War College, 2003
3. Brian P. Hamilton, **National Information Infrastructure: An Immediate Strategic Concern in National Security Policy.** Carlisle Barracks, PA, U.S. Army War College, 2004
4. Bonnie N Adkins, **The Spectrum of Cyber Conflict from Hacking to Information Warfare: What Is Law Enforcement's Role?** Maxwell AFB, AL, Air Command and Staff College, 2001
5. **Creation of a global culture of cybersecurity," Resolution adopted by the General Assembly"**, United Nations, Fifty-seventh session , Agenda item 84 (c), A/RES/57/23, 31 January 2003
6. **Diversification Of Cyber Threats , Trustees of Dartmouth College (Institute for Security Technology Studies).** U.S.Department of Justice. MAY 2002
7. **Emerging Cyber Threats Report for 2008,** Georgia Tech Information Security Center, October 2, 2007

8. **Information Security: Emerging Cyber security Issues Threaten Federal Information Systems.** Washington, GAO, May 2005.
9. **General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security**, UN document A/RES/53/70, 4 January 1999.
10. **General Assembly, Developments in the Field of Information and Telecommunications in the Context of InternationalSecurity**, UN document A/RES/56/19, 7 January 2002.
11. General Assembly, **Developments in the Field of Information and Telecommunications in the Context of InternationalSecurity**, UN document A/RES/61/54, 19 December 2006.
12. General Assembly, **Creation of a Global Culture of Cybersecurity**, UN document A/RES/57/239,31 See for example, General Assembly, **Creation of a Global Culture of Cybersecurity**, UN document A/RES/57/239, January 2003; and General Assembly, **Creation of a Global Culture of Cybersecurity and the protection of critical information infrastructures**, UN document A/RES/58/199, 30 January 2004.
13. **The Global Cybersecurity Agenda** (GCA), A Framework for International Cooperationin Cybersecurity, International Telecommunication Union (ITU),April ,2008
14. James E Barrineau. **Securing American Cyberspace: A Strategic Necessity.** Carlisle Barracks, PA, U.S. Army War College, 2004.
15. James B. Michael, **Phase II Report on Intelligent Software Decoys: Intelligent Software Decoy Tools for Cyber Counterintelligence and Security Countermeasures.** Monterey, CA, Naval Postgraduate School, April 28, 2004.
16. Jeffrey C. Sobel, **Digination: The Birth of Cyber-Nations.** Maxwell AFB, AL, Air Command and Staff College, 2005
17. Jennie M.Williamson, **Information Operations: Computer Network Attack in the 21st Century.** Carlisle Barracks, PA, U.S. Army War College, 2002.
18. Library of Congress. Congressional Research Service. **Information Operations and Cyber war: Capabilities and Related Policy Issues**, by Clay Wilson. Washington, CRS, September 14, 2006
19. **Securing Cyberspace for the 44th Presidency**, A Report of theCSIS Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies, US, Washington, DC,December 2008
20. Sonya Cox. **Cyber warfare: Ulysses Bow or Achilles Heel for the Combatant Commander?** Newport, RI, Naval War College, Joint Military Operations Department, 2004.
21. Thomas Wingfield. **An Introduction to Legal Aspects of Operations in Cyberspace.** Monterey, CA, Naval Postgraduate School, 2004
22. Todd A. Megill, **The Dark Fruit of Globalization: Hostile Use of the Internet.** Carlisle Barracks, PA, U.S. Army War College, 2005.
23. Timothy F. O'Hara, **Cyber Warfare/Cyber Terrorism.** Carlisle Barracks, PA, U.S. Army War College, 2004.
24. United States. General Accounting Office. **Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed.** Washington, GAO, 2002.
25. United States. Government Accountability Office. **Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cyber security Responsibilities**, by David A. Powner. Washington, GAO, 2005.
26. Philip B Erdie,**Network-Centric Strategic-Level Deception.** Monterey, CA, Naval Postgraduate School, 2004
27. Preamble of the Antarctic Treaty, text available at the National Science Foundation website: http://www.nsf.gov/od/opp/antarct/anttrty.jsp

**B: Official resources**

- **Books**

1. Alan D. Campen,. and Douglas H. Dearth, , eds. **Cyber war 2.0: Myths, Mysteries and Reality**. Fairfax, VA, AFCEA International Press, 1998
2. Alvin and Heidi Toffler " **Forword:the new intangibles ", in Athena s camp: preparing for conflict in the information age** ", edited by john arquilla & David ronfeldt ", Santa monica,ca:rand,1997
3. A.M. Chircu and R.J. Kauffman, **Strategies for Internet middlemen in the intermediation/disintermediation/reintermediation cycle,** Electronic Markets 9(1/2) (1999),
4. Athina Karatzogianni,(ed), "**Cyber-Conflict and Global Politics**"', Routledge and Taylor & Francis Group. , 11th September 2008
5. Amitav Mallik," **Technology and Security in the 21st Century** A Demand-side Perspective", SIPRI Research Reports, hardback, Nov 2004
6. Amir Dhia," **The Information Age and Diplomacy: An Emerging Strategic Vision in World Affairs**", Published by Universal-Publishers, 2006
7. Anthony H. Cordesman, and Cordesman, Justin G. **Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland.** Westport, CT, Praeger, 2002.
8. Arnold K. Veazie, **U.S. Strategy for Cyberspace**. Carlisle Barracks, PA, U.S. Army War College, 2003.
9. Arsenio T. Gumahad, **Cyber Troops and Net War: The Profession of Arms in the Information Age**. Maxwell AFB, AL: Air University, Air War College, April 1996.
10. Bill Hutchinson & Mat Warren ," **information warfare : corporate attack and defence in digital world** ", print edition typeset by Avocet typist , ,brill,Aylesbury,bucks,printed and bound in Great Britain, 2001
11. Brynjar Lia," **The Impact of Globalization on Future Patterns of Terrorism", Terrorism and Asymmetric Warfare Project**, Norwegian Defence Research Establishment (FFI), Presentation Oslo-Norway, ,OMS-Seminar 27 September 2000
12. ________, **Globalization and the Future of Terrorism: Patterns and Predictions** (London: Routledge, 2005
13. B.Wellman, "**Does the internet increase, decrease or supplement social capital?**" ,American behavioral Scientist ,45(3),2001
14. Bonnie N. Adkins, ," **The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?",** A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, Maxwell Air Force Base, Alabama, April 2001
15. Christophe Engel Kenneth H.Keller (eds.):**Understanding the Impact of Global Networks on Local Social, Political and Cultural Values**", Lorenz Muller ," Global Networks and Local Values" , Law and Economics of International Telecommunications [42]),Baden-Baden (Nomos) 2000
16. Craig A. Schiller and others. **Botnets: The Killer Web App**. Rockland, MA, Syngress Publishing, 2007
17. Craig A. Smith, " **The World Wide Web of War**", Strategy Research Project, U.S. Army War College, 21 February 2006
18. **Cyber Warfare and Cyber Terrorism,** edited by Lech J. Janczewski and Andrew M. Colarik. Hershey, PA, Information Science Reference, 2008
19. **Cyber media Go to War: Role of Converging Media during and after the 2003 Iraq War,** edited by Ralph D. Berenger. Spokane, WA, Marquette Books, 2006\
20. **Cyber war, Netwar and the Revolution in Military Affairs,** edited by Edward Halpin. New York, Palgrave Macmillan, 2006
21. D. Curtis. Schleher, **Electronic Warfare in the Information Age**. Boston, Artech House, 1999.
22. Daniel M. Gerstein, **Securing America's Future: National Strategy in the Information Age**. Westport, CT, Praeger Security International, 2005.
23. Dan Verton," **Black Ice: The Invisible Threat of Cyber-Terrorism.** New York, McGraw-Hill/Osborne, 2003
24. Daniel M. Vadnais," **Law Of Armed Conflict And Information Warfare — How Does The Rule Regarding : Reprisals Apply To An Information Warfare Attack?"** ,The Research Department ,Air Command and Staff College,

March 1997Darrel C. Menthe," JURISDICTION IN CYBERSPACE: A THEORY OF INTERNATIONAL SPACES", 4 Mich. Telecomm. Tech. L. Rev. 69 (1998)

25. David C. Gompert, Irving Lachow,and Justin Perkins," **Battle-Wise Seeking Time-InformationSuperiority in Networked Warfare**"Center for Technology and National Security Policy
, National Defense University Press, Washington, D.C.,2006
26. David J. Gruber," **Computer Networks and Information Warfare Implication for Military Operations**", Occasional Paper No. 17, Center for Strategy and Technology Air War College, July 2000
27. David S. Alberts,John J. Garstka,Richard E. Hayes, and David A. Signori," Understanding Information Age Warfare" Library of Congress Cataloging-in-Publication Data, August 2001
28. David J. Lonsdale, **the Nature of War in the Information Age: Clausewitzian Future.** New York, Frank Cass, 2004.
29. Dawn M. Gibson," **A VIRTUAL PANDORA'S BOX: ANTICIPATORY SELF-DEFENSE IN CYBERSPACE** ", 2004
30. Dorothy Denning & Elizabeth Robling. **Information Warfare and** Security. New York, ACM Press, 1999. Dorothy Denning, "Information Warfare and Cyber-terrorism," Women in International Security (WIIS) Seminar, Washington, D.C. (15 December 1999
31. Edward Halpin.(eds),Cyberwar, **Netwar and the Revolution in Military Affairs,** New York, Palgrave Macmillan, 2006
32. Ethan Gutmann, **Losing the New China: A Story of American Commerce, Desire and Betrayal,**San Francisco: Encounter Books, 2004
33. Eugene B. Skolnikoff," **Will Science and Technology Undermine the International Political System?**", the 2001 Loewy Memorial Lecture given at the Edmund A. Walsh School of Foreign Service, Georgetown University, Washington, DC, March 13, 2001
34. **Fighting Terror in Cyberspace,** edited by Mark Last and Abraham Kandel. Hackensack, NJ, World Scientific, 2005.
35. Hank T. Christen, James P. Denney & Paul M. Maniscalco, "**Weapons of Mass Effect: Cyber-Terrorism,**" in Paul M. Maniscalco & Hank T. Christen (Eds),
36. **Understanding Terrorism and Managing the Consequences** (New Jersey: PrenticeHall, 2002
37. Hoffman Bruce, **Responding to Terrorism Across the Technological Spectrum.** Carlisle Barracks, PA: Army War College, Strategic Studies Institute, 1994.
38. Gabriel Weimann, **Terror on the Internet: The New Arena, the New Challenges.** Washington, United States Institute of Peace Press, 2006
39. Grant Rebecca, **Victory in Cyberspace.** Arlington, VA, Air Force Association, 2007.
40. Guisnel Jean., **Cyber wars: Espionage on the Internet.** New York, Plenum Trade, 1997.
41. J.A. Lewis, **Assessing the risk of cyber terrorism,** cyber war and other cyber threats, Center for Strategic and International Studies ,2002
42. Jack L. Goldsmith and Tim. Wu, Who **Controls the Internet? Illusions of a Borderless World.** New York, Oxford University Press, 2006
43. James R. Blaker,. **Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare.** Westport, CT, Praeger Security International, 2007
44. James R. Hosek, "**The Soldier of the 21st Century,**" in New Challenges, New Tools for DefenseDecision making, (ed.) Stuart E. Johnson, Martin C. Libicki, and Gregory F. Treverton (Santa Monica,CA: RAND, 2003),
45. James M. Liepman, Jr.," **Cyberspace: The Third Domain**", Zel Technologies, LLC and Global Cyberspace Integration Center, November 15, 2007
46. **Jane's Radar and Electronic Warfare Systems 2007-2008.** Alexandria, VA, Jane's Information Group, 2007.
47. Jan A.G.M. van Dijk, **Models Of Democracy And Concepts Of Communication, Digital Democracy,** Issues Of Theory And Practice, Sage Publications Copyright, 2000

48. Jefferson D. Reynolds, **Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground,** 56 A.F. L. REV. 1 ,2005
49. Jeffrey C. Sobel, Divination: **The Birth of Cyber-Nations.** Maxwell AFB, AL, Air Command and Staff College, 2005
50. Jeremy W. Crampton, **The Political Mapping of Cyberspace.** Chicago, University of Chicago Press, 2003
51. Jerome C. Glenn and Theodore J. Gordon," **2004 State of the Future"**, Chapter 5,Technology, The Millennium Project American Council for the UNU., Millennium Project Publications,2004
52. Jennie M. Williamson,." **Information Operations: Computer Network Attack in the 21st Century**", Carlisle Barracks, PA, U.S. Army War College,2002.
53. John Arquilla, David Ronfeldt ,**Networks and Netwars: The Future of Terror, Crime, and Militancy**, RAND, 2001
54. john baylis and N.J.rengger (eds),"**dilemmas of world politics ,international issue in a changing world** ,oxford un.press inc.,Newyork ,1992
55. Johan Gearson " **the nature of modern terrorism**" the political quarterly publishing co.ltd .2002 ,USA,
56. John Arquilla and Ronfeldt, David. **Swarming & the Future of Conflict.** Rand, 2000.
57. Ulrich Beck," **Risk Society: Towards a New Modernity**", part 1 ," living on the volcano of civilization : contours on risk society " Sage Publications Ltd; 1 edition , 1992
58. John Arquilla and David F. Ronfeldt. **Cyber war is coming!** P-7791. Santa Monica, CA: Rand, 1992
59. ________. "**Cyber war is coming!**" p. 24-50, IN: Stocker, Gerfried and Christine Schopf (eds). Infowar. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998.
60. K.L. Hacker and J. van Dijk, **What is digital democracy?, in: Digital Democracy. Issues of Theory and Practice,** K.L.Hacker and J. van Dijk, eds, Sage Publications, London, 2000
61. Kath Wood ward, "**understanding identity** " , Oxford university press inc.2002
62. Knut Dörmann," **Computer network attack and international humanitarian law**", The Cambridge Review of International Affairs "Internet and State Security Forum", , Trinity College, Cambridge, UK,19 May 2001
63. Lawrence T. Greenberg &, Seymour E. Goodman &, Kevin J. Soo Hoo," **Information Warfare and International Law**", National Defense University Press, 1998
64. Lech Janczewski &Andrew M. Colarik , **Managerial Guide for Handling Cyber-Terrorism and Information Warfare,** Idea Group Publishing Hershey, PA, USA : 2005
65. ____________________,(eds)," **Cyber Warfare and Cyber Terrorism**" ,. Hershey, PA, Information Science Reference, 2008
66. LTC Bryan W. Ellis , ," The **International Legal Implications and Limitations of Information Warfare: What Are Our Options?**", USAWC STRATEGY RESEARCH PROJECT, U.S. Army War College, 2001
67. Lynn E.Davis, "**globalization's security implications**" ,Issue paper ,RAND,2003
68. Martin C. Libicki, **Conquest in Cyberspace: National Security and Information Warfare.** New York, Cambridge University Press, 2007
69. Mosco Vincent, the **Digital Sublime: Myth, Power, and Cyberspace.** Cambridge, MA, MIT Press, 2004.
70. Richard K. Betts, (editor), Robert O. Keobane & Joseph S Nye ," **power ,interdependence, and the information age** ", at ," conflict after the cold war :arguments on causes of war and peace ", second edition ,2002
71. Robert H. Anderson. And Anthony C. Hearn. **An Exploration of Cyberspace Security R&D Investment Strategies for DARPA**: "The Day after . . . in Cyberspace II." Santa Monica, CA: Rand, 1996.
72. Robert J. Bunker.," Five-Dimensional (Cyber) War fighting: Can the Army after Next Be Defeated by Technologies?" Carlisle Barracks, PA: Army War College, Strategic Studies Institute, 1998.

73. Rohas Nagpal," **Cyber Terrorism In The Context Of Globalization**", II World Congress on Informatics and Law,Madrid,Spain,September 2002
74. Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson," **Strategic Information Warfare: A New Face of War**", National Defense Research Institute, RAND Corporation, 1995,
75. S. Coleman, J. Taylor and W. van de Donk, (eds), **Parliament in the Age of the Internet**, Oxford University Press, Oxford,1999
76. S. Rafaeli., and, F. Sudweeks "**Interactivity on the nets in network and net play :virtual groups on the internet**, (eds) F.sudweeks and M.maclaughlim, Menlo park CA:mit press 1998
77. Sebastian M. Convertino and others. **Flying and Fighting in Cyberspace.** Maxwell Air Force Base, AL, Air University Press, 2007
78. Seymour E. Goodman & Abraham D. Sofaer, (eds) ," **THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM**" Ekaterina A. Drozdova," Civil Liberties and Security in Cyberspace" CHAPTER5 , the Board of Trustees of the Leland Stanford Junior University, 2001
79. Seymour E. Goodman and Herbert S. Lin (eds),"**Toward a Safer and More Secure Cyberspace**, Washington, National Academies Press, 2007
80. Shane P. Courville, Air **Force and the Cyberspace Mission: Defending the Air Force's Computer Networks in the Future.** Maxwell Air Force Base, AL, Center for Strategy and Technology, Air War College, 2007.
81. Steven Metz," **Armed Conflict In The 21st century:The Information Revolution And Post-Modern Warfare**", Strategic Studies Institute, U.S. Army War, April 2000
82. Thomas C. Wingfield &, James B. Michael," **An Introduction to Legal Aspects of Operations in Cyberspace**", Naval Postgraduate School Homeland Security, Monterey, California, 28 April 2004,
83. Tim Jordan," **Cyber power: The Culture and Politics of Cyberspace and the Internet**", Routledge, 2000
84. Timothy L. Thomas, **Cyber Silhouettes: Shadows over Information Operations.** Fort Leavenworth, KS, Foreign Military Studies Office, 2005.
85. Todd A. Megill, **The Dark Fruit of Globalization: Hostile Use of the Internet.** Carlisle Barracks, PA, U.S. Army War College, 2005
86. **Toward a Safer and More Secure Cyberspace**, edited by Seymour E. Goodman and Herbert S. Lin. Washington, National Academies Press, 2007
87. K.L. Hacker and J. van Dijk, **What is digital democracy? in: Digital Democracy. Issues of Theory and Practice**, K.L.Hacker and J. van Dijk, eds, Sage Publications, London, 2000
88. Kasia Wichrowska , **Advancements in Information and Technology and International Security** ,North American Model United Nation 2006, ,
89. Kath Wood ward, "**understanding identity** " chapter 5"emboding identity ", Oxford university press inc. 2002,
90. Paul.Levinson, **Realspace: The Fate of Physical Presence in the Digital Age, on and off Planet.** New York, 2003. .
91. T. G. Lewis, **Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.** Hoboken, NJ, Wiley-Interscience, 2006.
92. Stephen J. Lukasik and others. **Protecting Critical Infrastructures Against Cyber-Attack.** New York, Oxford University Press, 2003
93. Steven Metz," **Armed Conflict In The 21st Century:The Information Revolution And Post-Modern Warfare** ", Strategic Studies Institute, U.S. Army War, , April 2000
94. Richard K.Betts, (editor), "**conflict after the cold war: arguments on causes of war and peace** ", second edition, 2002,
95. Roger C. Molander , , Riddile, Andrew S., and Peter A. Wilson," **Strategic Information Warfare: A New Face of War**", National Defense Research Institute, RAND Corporation, 1995
96. Pippa Norris .," **Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide**, Part II. The Virtual Political System: chapter 5 " Theories of digital democracy,", Cambridge University Press, 2001,
97. J. P. Robins, "**Military Adventures in Cyberspace.**" **IN: Proceedings of the Second International Symposium on Command and Control Research and**

**Technology.** Market Bosworth, United Kingdom, 24-26 June 1996. Washington, DC: National Defense University, 1997.

98. Patrick D. Allen, **Information Operations Planning**. Norwood, MA, Artech House, 2007
99. Philip M. Seib, **Beyond the Front Lines: How the News Media Cover a World Shaped by War.** 1st ed. New York, Palgrave Macmillan, 2004.. See chapter titled, "Cyber news, Cyber war: The Internet as Tool and Battleground.
100. **Strategic Appraisal: The Changing Role of Information in Warfare**, edited by Zalmay M. Khalilzad and others. Santa Monica, CA, RAND, 1999
101. U.S. National Research Council. Committee on Counterterrorism Challenges for Russia and the United States. **Terrorism: Reducing Vulnerabilities and Improving Responses.** Washington, National Academies Press, 2004. "A collection of 22 papers on urban terrorism, cyberterrorism, and related topics."
102. United States. Assistant Secretary of Defense for Command, Control Communications and Intelligence. **Electromagnetic Spectrum Management Strategic Plan.** Washington, Department of Defense, 2002..
103. United States. Department of Homeland Security. **National Infrastructure Protection Plan.** Washington, U.S. Department of Homeland Security, 2006..
104. Vincent Moscow, **The Digital Sublime: Myth, Power, and Cyberspace.** Cambridge, MA, MIT Press, 2004.
105. Verton Dan, Black **Ice: The Invisible Threat of Cyber-Terrorism**. New York, McGraw-Hill/Osborne, 2003
106. Willis H. Ware, **the Cyber-Posture of the National Information Infrastructure.** Santa Monica, CA: Rand, 1998.
107. Walter Gary Sharp ", **Cyberspace and the Use of Force** ,"Ageis Research Corp ,February 1, 1999
108. Yonah Alexander and Donald J. Musch (eds.) **Cyber Terrorism and Information Warfare.** Dobbs Ferry, NY: Oceana Publications, 1999

- **Periodicals**

1. Alexander Spencer, Questioning the Concept of 'New Terrorism 'Peace Conflict & Development, Issue 8, January 2006
2. Andreas Wenger ," The Internet and the Changing Face of International Relations and Security", Information & Security, an international journal , ProCon Ltd., Sofia, Bulgaria , Volume 7, 2001
3. Anatolij A Streltsov," International Information Security: Description and Legal Aspects",ICTs and International Security , United Nations Institute for Disarmament Research (UNIDIR), Geneva, 2007
4. Antonio Nucci, and Steve Bannerman,. Controlled Chaos. IEEE Spectrum 44:43-48 December 2007.
5. Anthony M. Helm,(ed) " The Law of War in the 21st Century: Weaponry and the Use of Force", International Law Studies, Volume 82, Naval War College Newport, Rhode Island 2006
6. B. Wellman,"Does the internet increase, decrease or supplement social capital?" American behavioral Scientist ,45(3),2001
7. Bradley K. Ashley, The United States Is Vulnerable to Cyber terrorism. Signal 58:61-64 March 2004.
8. Bruce D. Berkowitz, War Logs On. Foreign Affairs 79:8-12 May-June 2000.
9. Bourque Jesse , the Language of Engagement Influence and the Objective. Journal of Electronic Defense 30:30-35 November 2007
10. China's Cyber warriors. Foreign Policy September-October: 93 2006.
11. Colonel Robert E. Schwarze, USAF Chief, Electronic Warfare and Cyber warfare Division, Headquarters U.S. Air Force. Journal of Electronic Defense 30:30-31 April 2007.
12. Charles E. Jr. Croom, Guarding Cyberspace: Global Network Operations. Joint Force Quarterly No. 46:68-69 2007.
13. CPT Ow Kim Meng, Cyber-Terrorism: An Emerging Security Threat Of The New Millennium , POINTER, the official journal of the Singapore Armed Forces, V28 N3, Jul - Sep 2002

14. David G. Post," a against "a against cyber anarchy" Berkeley university,US,vol.7, ,2002
15. David A. Fulghum, Subtle Wars. Aviation Week & Space Technology 166:126-127 June 18, 2007.
16. ___________, and Barrie, Douglas. Searching for Weakness. Aviation Week & Space Technology 166:26-27 April 30, 2007.
17. David Bond, Cyber Pork: Air Force Looks for a Cyberspace Home. Aviation Week & Space Technology 167:27 September 3, 2007.
18. David W. Munns, the Cyber Dilemma. Sea Power 50:50-52 May 2007.
19. David A. Umphress, Cyberspace: The New Air and Space? Air & Space Power Journal 21:50-55 springs 2007
20. Duncan B. Hollis," Why States Need an International Law for Information Operations ", Lewis & Clark Law Review, Vol. 11, p. 1023, 2007
21. Dimitrios Delibasis," State Use of Force in Cyberspace for Self-Defence:A New Challenge for a New Century" , Peace Conflict and Development: An Interdisciplinary Journal, Issue 8, February 2006,
22. Don. Tennant Climate Changers. Computerworld 41:20 June 11, 2006.
23. Graham E. Fuller, Islamist Politics in Iraq after Saddam Hussein, The United States Institute of Peace. Special Report No. 108, August 2003
24. Electromagnetic Spectrum: Critical to Our Nation's Security and Economy. CHIPS 25:29-30 January-March 2007
25. Florian Bieber, Cyber war or Sideshow? The Internet and the Balkan Wars. Current History 99:124-128 March 2000.
26. G. Pye and M. J. Warren, Modeling Critical Infrastructure Systems. Journal of Information Warfare No. 6: March 2007. pp41-53
27. Henning Wegener , " Harnessing the perils in cyberspace: who is in charge?", Disarmament fourm , icts and international security , three ,2007
28. James Adams, Virtual Defense. Foreign Affairs 80:98-112 May-June 2001.
29. Air Force Establishes Provisional Command for Cyberspace. Defense Daily 235: September 19, 2007.
30. James Mulvenon ," Toward a Cyberconflict Studies Research Agenda",in "On the Horizon",O.sami Saydijari,(editor), IEEE computer security ,july/august 2005
31. K. Chaisson, China Report Looks at "Informationization". Journal of Electronic Defense 30:20 July 2007.
32. K.Webb, Information Terrorism in the New Security Environment. Journal of Information Warfare 6:15-24 August 2007
33. Keith B. Alexander, War fighting in Cyberspace. Joint Force Quarterly No. 46:58-61 2007.
34. Patrick D. Allen and Chris C. Demchak, the Palestinian-Israeli cyberwar. Military Review 83:52-59 March-April 2003.
35. Cullather Nick, Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyber war. Intelligence & National Security 18:141-154 Winter 2003.'
36. Harrington Caitlin. USAF Explores Doctrine for Cyber Warfare. Jane's Defence Weekly 45:10 January 2, 2008.
37. James Adams ,virtual defense "Foreign Affairs",vol.80,No.3,may/june 2001
38. John M. Doyle, COIN of the Realm. Aviation Week & Space Technology 165:122 October 23, 2006.
39. Jeremy Pressman," Rethinking Transnational Counterterrorism ", The Washington Quartery,Vol.,30,No.4,Autumn 2007
40. Johan Gearson " the nature of modern terrorism" the political quarterly publishing co.ltd .2002 ,USA
41. Joshua Green. "The myth of cyber terrorism" ,Washington monthly ,November 2002
42. Journal of Homeland Security and Emergency Management: , Volume 2 Issue 4,2005
43. John C. Koziol, Contesting the Information Battlespace. Joint Force Quarterly No. 46:71 2007..
44. Karine Barzili-Nahon ," Cultured Technology : the internet and religious fundamentalism ,The information society",Taylor&Farncis group,volume21 ,number 1 , Jan –Mar. 2005
45. Khine. Latt, Future Naval Supremacy. Military Technology 31, 2007

46. Matthew J. Morgan," The Origins of the New Terrorism", Parameters, Vol. 34, Spring 2004
47. Michael N Schmitt," , War, Technology and the Law of Armed Conflict", International Law studies, Volume 82, Naval War College Newport, Rhode Island 2006
48. ____________" Wired warfare: Computer network attack and jus in bello , RICR Juin IRRC June, Vol. 84 No 846, 2002
49. ____________, Computer networks Attack and the use of force in International law: thoughts on a normative Framework ", The Columbia Journal of Transnational Law, Volume 37, 1999,
50. Mark Russell Schulman ,"legal constraints on information warfare", Occasional paper, No.7, center for strategy and technology ,air war college ,March 1999
51. Myriam A. Dunn," The Cyberspace Dimension in Armed Conflict", Information and Security, An International Journal, Vol. 7, 2001
52. ____________," The Internet and the Changing Face of International Relations and Security", Volume number: 7, Issue number: 1, ProCon Ltd., Sofia, Bulgaria, 2001
53. ____________, " Information Age Conflicts :A Study of the Information Revolution and a Changing Operating Environment", Center for Security Studies (CSS), ETH Zurich, Issue No. 64, 2002
54. ____________,Towards an International Regime for the Protection of Cyberspace?", CIIP Research Group, Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology), Switzerland, Volume 2, Number 11 , May 2004
55. New Global Partnership to Fight Cyber Terrorism Seeks the Business,, Zeichner Risk Assessment Newsletters , " Vol. 1, No. 30 - May 30, 2008
56. Paul D. Berg, Dominant Air, Space, and Cyberspace Operations. Air & Space Power Journal 21:30-31 springs 2007.
57. Paul W. Phister and others. The "Cyber Craft" Concept. Military Technology 31:123 September 2007.
58. Ph. E. Agre, Real-Time Politics: The Internet and the political process, The Information Society 18 (2002
59. Rosine Matthew., Deciphering Cyberspace. Airman 51:10-15 Fall 2007.
60. Robert McMillan,. Is the U.S. at Risk from Cyber warfare? PC World 25:53 October 2007
61. Robert N. Charette, Open-Source Warfare. IEEE Spectrum 44:26-32 November 2007.
62. Susan W. Brenner, "At Light Speed": Attribution and Response to Cybercrime. Journal of Criminal Law & Criminology 97:379-475 Winter 2007.
63. Shorer-Zeltser, M. and Ben-Israel, G. M. Religious Internet Networks and Mobilization to Terror. Journal of Information Warfare 6:1-14 August 2007.
64. Sheryl J. Brown and Margarita S. Studemeister "Virtual Diplomacy: Rethinking Foreign Policy Practice in the Information Age ",Information & Security. Volume 7, 2001The DON Electromagnetic Spectrum Campaign Plan. CHIPS 25:21 July-September 2007..
65. Robert Klepper, "The World Wide Web as Mass Medium," Information Strategy 14 (Fall1997): 1 [database on-line]; available from Wilson Web; accessed 18 January 2006.
66. Renee de Never," Modernizing the Geneva Conventions", The Washington Quarterly, Vol. 29, No. 2 Spring 2006
67. Thomas Mockaitis," The "New" Terrorism: Myths and Reality", Middle East Quarterly VOL,XIV,No, 4, Fall 2007
68. Timoyhy L. Thomas , "Chines American Network Warfare", Joint Force Quarterly, USA , Issue 38, 2005
69. L. Walsh. and J. Barbara," Speed, international security, and "new war" coverage in cyberspace". Journal of Computer-Mediated Communication, *12*(1), article 10.. (2006)
70. Martin R. Stytz, Cyber-warfare Distributed Training. Military Technology 30:95-99 2006.
71. Technology of Networked Control Systems. Proceedings of the IEEE 95: entire issue January 2007.
72. N. C. Rowe, War Crimes from Cyber-weapons. Journal of Information Warfare 6:15-25 December 2007.

73. U. Josefsson and A. Ranerup, Consumerism revisited: the emergent roles of new electronic intermediaries between citizens and the public sector, Information Polity 8 (2003
74. Vijayan Jaikumar., Lack of Leadership Hampers Cyber security Efforts, Say Critics. Computerworld 40:16 September 18, 2006.
75. Wagner Breanne., Electronic Attackers. National Defense 92:24-26 October 2007.
76. Wang Baocun and Li Fei," Information Warfare" Liberation Army Daily, June 13 and June 20, 1995
77. Wolf Walter., Information - The Fabric of Cyberspace, Journal of Electronic Defense 30:12.

- **Reportes**

1. Adam Peake, **Internet governance and the World Summit on the Information Society (WSIS)- Prepared for the Association for Progressive Communications** (APC) June 2004
2. Clay Wilson," **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress**",Congressional Research Service, January 29, 2008
3. Craig A. Smith," **The World Wide Web of War**", Strategy Research Project, U.S. Army War College, 21 February 2006
4. Eugene B. Skolnikoff," **Will Science and Technology Undermine the International Political System**", the 2001 Loewy Memorial Lecture given at the Edmund A. Walsh School of Foreign Service, Georgetown University, Washington, DC, March 13, 2001
5. Gabriel Weimann, "**How Modern Terrorism Uses the Internet**, The United States Institute of Peace, www.terror.net, Special Report No. 116, March 2004
6. ____________,**Cyber terrorism: How Real Is the Threat?"**, The United States Institute of Peace,, Special Report No. 119, December 2004
7. -___________, **Cyber terrorism: How Real Is the Threat?**, The United States Institute of Peace,, Special Report No. 119, December 2004
8. Kevin G. Coleman, **A Cyber War has begun, Cyber Warfare,** ***The Technolytics Institute***, *September 2007*(http://www.technolytics.com/Technolytics_Cyber_War.pdf)
9. Richard Solomon," **The Global Information Revolution and International Conflict Management**", United States Institute of Peace, virtual diplomacy report, VDS No. 17,January 2004
10. **Towards: knowledge societies** , unesco world report ,unesco, 2005
11. J.A Lewis,, **Assessing the risk of cyber terrorism, cyber war and other cyber threats,** Center for Strategic and International Studies, (2002
12. **Information Warfare and the Air Force: Wave of the Future? Current Fad?"**, RAND, March 1996
13. **On the Unlawfulness of the Use and Threat of Nuclear Weapons,** Report of the Foreign and International Law Committee of the New York County Lawyers' Association, available at: http://www.nuclearweaponslaw.com/JournalsReport/NYCLA_Report.pdf. Last visited: Feb. 24, 2008

- **Newspapers**

1. Kathryn Kerr," **Putting cyberterrorism into context"**, Auscert,24 October 2003
2. Scott Berinato ,**the trust about Cyberterrorism,** CIO Magazine ,15 Mar.2002
3. **Greece arrests man suspected of major data hacks**,Reuters, January 25, 2008
4. Adam Roberts," **The Changing Faces of Terrorism**", BBC History: 2002-08-27
5. Ellen Nakashima," **Bush Order Expands Network Monitoring**", Washington post, .27-1-2008
6. Martin Asser," **Israel army in Face book clampdown** ",bbc news, 11 April 2008
7. Ilya Kramnik," **Cyberspace Wars: Militarization of Virtual Front**", Moscow, News,22/05/2008
8. Tom Espiner," CIA: **Cyberattack caused multiple-city**",Special to CNET News.com,January 22, 2008

9. Liam Tung, **China accused of cyberattacks on New Zealand**," Special to CNET News.com, September 13, 2007
10. Robert Vamosi, **Cyber attack in Estonia--what it really means**, Special to CNET News.com, May 29, 2007
11. China 'hacked' into Pentagon defense system, The Financial Times, September 4 2007
12. **Cyber security beware the Trojan panda**, the Economist, sept. 8th-14th 2007 pp58
13. Bill Gertz, **"China's Spies 'Very Aggressive' Threat to U.S.,"** The Washington Times, March 6, 2007,
14. **For an overview of China's cyber war strategies**, see James C. Mulvenon, **"Chinese Information Operations Strategies in a Taiwan Contingency,"** testimony before the U.S.–China Economic and Security Commission, September 15, 2005
15. **"Pentagon Developing Cyberspace Weapons,"** Washington Technology, June 22, 1995.
16. Ellen Nakashima," **Bush Order Expands Network Monitoring**", washingtonpost.27-1-2008
17. John J. Tkacik, Jr.," **Trojan Dragon: China's Cyber Threat**", The Heritage Foundation
18. , No. 2106, February 8, 2008
19. **U.S.–China Economic and Security Review Commission,** 2007 Report to Congress, November 2007, p. 7,
20. Johan Markoff," **Internet Traffic Begins to Bypass the U.S.**", New York Times , August 29, 2008
21. Dow Jones Newswires, **"Taiwan Military—China Cyber War More Likely Than Invasion,"** December 14, 2004;
22. **"Chinese Hacker May Be PLA,"** Chosun Ilbo, July 15, 2004;
23. **"NK Hands Suspected in Cyber attacks,"** Korea Times, July 15,2004; Nautilus Institute, **"ROK Cyber attacks,"** July 15, 2004,
24. **"China Blamed for Cyber Sabotage in S Korea,"** Financial Times, May 3, 2005,
25. **"Flaw in Microsoft Word Used in Computer Attack,"** The New York Times, May 20, 2006, at
26. Rory McCarthy ," **Israel-Palestine dispute moves on to Facebook**", The Guardian, March 20 2008
27. David Shamah ," **Digital World: Israel or 'Palestine'?**" The Jerusalem Post , Mar 18, 2008,
28. **"Estonia Sees Red in Cyber attacks,"** IOL Technology, May 16, 2007.
29. **"Cyber Attacks Force Estonian Bank to Close Website,"** Agence France Presse, May 16, 2007.
30. "Peter Finn, **"Cyber Assaults on Estonia Typify a New Battle Tactic,"** Washington Post, May 19, 2007.
31. Robert Vamosi," **Cyberattack in Estonia--what it really means**" , Special to CNET News.com, May 29, 2007., Ian Traynor, Russia accused of unleashing cyber war to disable Estonia, THE GUARDIAN, May 17, 2007
32. Mark Landler and John Markoff," **In Estonia, what may be the first war in cyberspace**", International Herald Tribune , Monday, May 28, 2007
33. Shaun Waterman, **Who was behind Estonia's cyber attack?**, WORLD PEACE HERALD, Jun. 11, 2007. Nathaniel Hoopes , **New focus on cyber terrorism** ,CSmonitor ,15 August 2005 www.CSmonotir.com
34. Tom Espiner," **Georgia accuses Russia of coordinated cyber attack**", cnit, news, August 11, 2008
35. Kevin Coleman," **Cyber War 2.0 -- Russia v. Georgia**", defensetech.org, August 13, 2008
36. Ben Arnoldy," **Cyberspace: New Frontier in Conflicts**, .ABC News. August 1٧, 2008
37. Bradley Graham, **"Military Grappling with Guidelines for Cyber Warfare; Questions Prevented Use on Yugoslavia,"** The Washington Post, 8 November 1999,
38. Clara Moskowitz ," **Internet Full of 'Black Holes'**", .livescience.com, 2008-04-11

39. John Blau, "**US military plans to put Internet router in space**", IDG News Services, April 12, 2007
40. U.S. Military to Put Internet Router in Space, SPACE.com staff", 13 April 2007
Amoroso, Edward G. **Cyber Security**. Summit, NJ, Silicon Press, 2007
41. Kevin Paulsen ,."**UN warns of nuclear cyber attack risk**" , security focus , 27-9-2004
42. ,Nick Heath," Nato: **Cyber terrorism 'as dangerous as missile attack'**" silicon.com, 7 March 2008,
43. Nick Heath," **Nato allies form cyber defence command**, silicon.com, 8 April 2008
44. Greg Jaffe, "Gates Urges NATO Ministers to Defend Against Cyber Attacks," Wall Street Journal, June 15, 2007.
45. .Newly Nasty. **Economist** 383:63-64 May 26, 2007.

- **Internet Resources**

1. Cyber Terrorism Resource Centre Provides to links to article and commentaries around the world. http://www.globaldisaster.org/cyberterrorrescen.shtml
2. Internet / Network Security Resource guide on Cyber terrorism Listing of websites and articles http://netsecurity.about.com/cs/cyberterrorism/
3. National Cyber Security Alliance http://www.staysafeonline.info/
4. Information about the Air Force Cyber Command. **Available online at: http://www.afcyber.af.mil/**
5. Parry Aftab, The PR Professional's Role in Handling Cyber warfare. **Public Relations Strategist** 11:28 Summer 2005.
**Available online at: http://proquest.umi.com/pqdweb?did=885859521&Fmt=7&clientId=417&RQT=309&VName=PQD**
6. Air Force Institute of Technology. **Center for Cyberspace Research.**
**Available online at: http://www.afit.edu/ccr/**
7. Air War College Gateway. **Cyberspace and Information Operations Study Center.Available online at: http://www.au.af.mil/info-ops/index.htm**
8. Sam Atwood, Cyberspace **as a Theater of Conflict: Federal Law, National Strategy and the Departments of Defense and Homeland Security.** Wright-Patterson AFB, OH, Air Force Institute of Technology, Graduate School of Engineering and Management, June 2007
**Available online at: http://handle.dtic.mil/100.2/ADA471536**
9. Assistant Secretary of Defense, Networks and Information Integration. **Department of Defense Net-Centric Spectrum Management Strategy**, by John G. Grimes. Arlington, VA, August 3, 2006.
**Available online at: http://handle.dtic.mil/100.2/ADA454462**"
10. Calculating Cyber Attack Threats. **Scientific Computing** 24:10 March 2007.
**Available online at: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=24467546&site=ehost-live**
11. Cyber Attacks During the War on Terrorism: A Predictive Analysis Sept 2002 prepared by the Dartmouth Institute for Security Technology Studies in the US *Available online at: http://www.globaldisaster.org/cyberattacks.pdf*
12. Cyber Terrorism Resource Centre Provides to links to article and commentaries around the world. http://www.globaldisaster.org/cyberterrorrescen.shtml
13. **Cyber Storm Exercise.** Department of Homeland Security, September 2006.
**Available online at: http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm**
Includes Fact Sheet and Exercise Report.
14. **Defense Spectrum Organization. Available online at: http://www.disa.mil/dso/index.html**"
15. Department of Homeland Security Cyber Security. **NIPP-Cyber Security: Implementing the National Infrastructure Protection Plan.**
**Available online at: http://www.us-cert.gov/reading_room/infosheet_NIPP.pdf**

16. Matthew G. Devost, and Neal A. Pollard, Taking Cyber terrorism seriously. June 27, 2002.**Available online at:**
**http://www.terrorism.com/modules.php?op=modload&name=Documents&file=get&download=21**
"Failing to adapt to emerging threats could have dire consequences." **DIME: Information as Power. Available online at:**
**http://www.carlisle.army.mil/dime/**
17. Karol.Dobrzeniecki, How Should We Deal with Human Rights in Cyberspace? **International Review of Law, Computers & Technology** 19:253-258 November 2005.**Available online at:**
**http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=18945553&site=ehost-live**
18. David T. Fahrenkrug, the Age of Cyber Warfare. **The Wright Stuff** November 29, 2007.**Available online at:**
**http://www.maxwell.af.mil/au/aunews/archive/0222/Articles/TheAgeofCyberWarfare.html**
19. David T. Fahrenkrug, **Cyberspace Defined. Available online at:**
**http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html**
20. Sharon Gaudin and Larry Greenemeier, Cyberwarfare: A Realistic Appraisal. **InformationWeek** No. 1141:49 June 2007.
**Available online at:**
**http://proquest.umi.com/pqdweb?did=1288835551&Fmt=7&clientId=417&RQT=309&VName=PQD**
21. **Global Cyberspace Integration Center.**
**Available online at: http://www.gcic.af.mil/**
22. Larry.Greenemeier, Cyber warfare: By Whatever Name, It's on the Increase. **InformationWeek** No. 1145:32 July 2-9, 2007.**Available online at:**
**http://proquest.umi.com/pqdweb?did=1304891351&Fmt=7&clientId=417&RQT=309&VName=PQD**
23. Forrest B. Hare, Air Force Strategy for Cyberspace. **The Wright Stuff** November 29, 2007.**Available online at:**
http://www.maxwell.af.mil/au/aunews/archive/0222/Articles/strategy%20for%20cyberspace%20essay%20v3.pdf
24. William Heisey and others. **Automated Spectrum Plan Advisor for On-the-Move Networks.** October 2006.**Available online at:**
**http://handle.dtic.mil/100.2/ADA470331**
25. **Information Operations,** compiled by Debra Alexander. Maxwell AFB, AL, Muir S. Fairchild Research Information Center, August 2006. 28 p.
**Available online at: http://www.au.af.mil/au/aul/bibs/informops.htm**
26. Internet / Network Security Resource guide on Cyber terrorism Listing of websites and articles http://netsecurity.about.com/cs/cyberterrorism
27. IWS United Kingdom Website Listing Essential documents, articles, news watch, conferences and related links, as they apply to cyberterrorism.http://www.iwar.org.uk/cyberterror/index.htm
28. **Letter to Airmen: Cyberspace Operations.** May 7, 2007.
**Available online at:**
**http://www.af.mil/library/viewpoints/secaf.asp?id=320**
Honorable Michael W. Wynne, Secretary of the Air Force.
29. Library of Congress. Congressional Research Service. **Information Operations, Electronic Warfare, and Cyber war: Capabilities and Related Policy Issues,** by Clay Wilson. Washington, CRS, March 20, 2007.
**Available online at: http://handle.dtic.mil/100.2/ADA466599**
٣٠. James M. Jr. Liepman, Cyberspace: The Third Domain. **The Wright Stuff** December 13, 2007.**Available online at:**
**http://www.maxwell.af.mil/au/aunews/archive/0223/Articles/Cyberspace%20Third%20Domain%20-%20Liepman.pdf**
31. Sze Li Harry Lim, **Assessing the Effect of Honey pots on Cyber-Attackers.** Monterey, CA, Naval Postgraduate School, 2006. 63 p.
**Available online at: http://handle.dtic.mil/100.2/ADA462526**

32. **America's Edge: Cyberspace. Maintaining**
**Available online at:**
**http://www.posturestatement.hq.af.mil/1_2_intro.htm**
2007 U.S. Air Force Posture Statement.
33. Marquand, Robert and Arnoldy, Ben. China Emerges as Leader in Cyber warfare. **Christian Science Monitor** 99:1-4 September 14, 2007.
**Available online at:**
**http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=26595472&site=ehost-live**
34. Carolyn Duffy. Marsan, How Close Is World War 3.0? **Network World** 24:1-25 August 27, 2007.**Available online at:**
**http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=26383191&site=ehost-live**
35. Robert F. Mills, **Developing Cyberspace Competencies for Air Force Professional Military Education.Available online at:**
**http://www.oft.osd.mil/library/library_files/document_413_Cyber%20PME%20v2.pdf**
36. National Cyber Security Alliance http://www.staysafeonline.info/
37. **Technology and Terrorism: The New Threat for the Millennium** - Leamington Spa, UK: RISCT. 24 p. Author(s): Bowers, Stephen R., Keys, Kimberly R DC: Cyber terror and Other Prophecies Ed Frauenheim, Staff Writer, CNET News.com ,December 12, 2002
Available online at: http://news.com.com/2100-1001-977780.html?tag=fd_top
38. The Mouse That Roared. **Global Agenda** September 15, 2007.
**Available online at:**
**http://search.ebscohost.com/login.aspx?direct=true&db=f5h&AN=26566861&site=ehost-live**
39. Suzanne C. Nielsen, and, Donald Welch, Teaching Strategy and Security in Cyberspace: An Interdisciplinary Approach. **International Studies Perspectives** 4:133-144 May 2003.
**Available online at:**
**http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=9925418&site=ehost-live**
40. Office of the Assistant Secretary of Defense for Networks and Information Integration. **Department of Defense Electromagnetic Spectrum Management Strategic Plan.** Washington May 2007.**Available online at:**
**http://handle.dtic.mil/100.2/ADA470338**
41. Richard A. Radice, **Dominating Cyberspace.** Carlisle Barracks, PA, Army War College, March 12, 2007.
**Available online at: http://handle.dtic.mil/100.2/ADA468855.**
42. Gary Sevounts, Addressing Cyber Security in the Oil and Gas Industry. **Pipeline & Gas Journal** 233:79-80 March 2006.
**Available online at:http://search.ebscohost.com/login.aspx?direct=true&db=f5h&AN=20290236&site=ehost-live**
43. Sholtis Tadd., Cyberspace's Future: Influence Operations? **The Wright Stuff** November 29, 2007.**Available online at:**
**http://www.maxwell.af.mil/au/aunews/archive/0222/Articles/CyberspacesFutureInfluenceOperations.html**
44. Stephens Hampton., War in the Third Domain. **Air Force Magazine Online** April 2007.**Available online at:**
**http://www.afa.org/magazine/april2007/0407war.asp**
45. Martin R. Stytz and, Sheila B. Banks, **Issues and Requirements for Cyber security in Network Centric Warfare.** June 2004. **Available online at:**
**http://handle.dtic.mil/100.2/ADA466069**
46. Richard Solomon, ," The Global Information Revolution and International Conflict Management", United States Institute of Peace,
http://www.usip.org/virtualdiplomacy/publications/papers/rhsvd.htm
47. Terrorism Questions and Answers: Cyber terrorism Council on Foreign relations
http://www.terrorismanswers.com/terrorism/cyberterrorism.html

48. Timothy L. Thomas, **Hezbollah, Israel, and Cyber PSYOP.** Leavenworth, KS, U.S. Army Foreign Military Studies Office, 2007
**Available online at:** http://handle.dtic.mil/100.2/ADA465336
49. United States. Department of Homeland Security. **National Cyber Security Division. Available online at:** http://www.dhs.gov/xabout/structure/editorial_0839.shtm.
50. United States. Department of Homeland Security. **Protecting America's Critical Infrastructure - Cyber Security. Available online at:** http://www.us-cert.gov/press_room/050215cybersec.html
51. Fact sheet. United States. Joint Chiefs of Staff. **Joint Publication 3-13: Information Operations.** February 13, 2006.
**Available online at:** http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf
52. Clay Wilson," **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress**", Congressional Research Service, **January 29, 2008** http://italy.usembassy.gov/pdf/other/RL32114.pdf
53. Pamela L. Woolley **Defining Cyberspace as a United States Air Force Mission.** Wright-Patterson AFB, OH, Air Force Institute of Technology, School of Engineering and Management, June 2006. **Available online at:** http://handle.dtic.mil/100.2/ADA453972.

**Others:**

- **Conferences**

1. Alan J. Rosenblatt," International Relations in Cyberspace", presentation at the 40th annual meeting of the International Studies Association, Washington, D.C., February 16–20, 1999
2. Barry C. Collin, The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge11th Annual International Symposium on Criminal Justice Issues, Institute for Security and Intelligence
3. Rohas Nagpal," Cyber terrorism in the context of globalization ", II World Congress on Informatics and Law,Madrid,Spain,September 2002
4. William yurciik & David doss ," internet attacks: a policy framework for rules of engagement ",29th Annual Telecommunications Policy Research Conference (TPRC), MIT Press, 2001
5. Alan J.Rosenblatt," International Relations in Cyberspace", presentation at the 40th annual meeting of the International Studies Association, Washington, D.C., February 16–20, 1999
6. Stein Schjolberg, Chief Judge, Moss Tingrett Court, Norway. "Law Comes to Cyberspace," A presentation at the 11th UN Criminal Congress, Bangkok, Thailand. Workshop 6: Measures to combat computer-related crime. Apr. 18-25, 2007
7. Jaak Aaviksoo, Estonian Minister of Defense, "Cyber Defense—the Unnoticed Third World War," Address to the 24th International Workshop on Global Security, Paris, June 16, 2007.

الاسم : عادل عبد الصادق محمد الجخه
محل الميلاد : المنوفية
الجنسية : مصري

# " أثر الإرهاب الالكتروني على مبدأ استخدام القوة في العلاقات الدولية "

المشرف : أ.د أحمد عبد الونيس شتا (٢٠١٦ - ٢٠١٧)

## الملخص

كان لظاهرة الفضاء الالكتروني تداعياتها الايجابية على المجتمع الدولي ومثلت تطورا هاما من تطور المجتمع الدولي ، وفي نفس الوقت عكست تلك الظاهرة تزايد لدورها مع زيادة الاعتماد الدولي عليها في كافة الاصعدة السياسية والاقتصادية والامنية والثقافية وغيرها ، بشكل يعكس ظاهرة متعددة الابعاد تحوي مصالح الكترونية وفي نفس الوقت تتعرض لاخطار الكترونية وكان للثورة التكنولوجية وظهور مجتمع المخاطر في النظام الدولي ، واصبح هناك طابع الكتروني للأمن والقوة والصراع في النظام الدولي ،و أثر الفضاء الالكتروني على التفاعلات السياسية الدولية والتحول الديموقراطي . وفي الفصل الثاني اكد الباحث على الرغم من تميز الإرهاب الالكتروني في مفهومة وخصائصه والياته إلا انه يثير مجموعه أخرى من المفاهيم والتي ان اختلفت عن الارهاب الالكتروني فانها –في الوقت ذاته– ترتبط بدرجة او باخرى .

وفي الفصل الثالث يتم تناول دور الفضاء الالكتروني في التأثير على طبيعة الصراع و القوة التي تمارس من خلاله بالإضافة إلى طبيعة النتائج والآثار التي تنتج عنه ، وهذا ما يعبر عن نوع جديد من ممارسة القوة وعمليات الهجوم والدفاع عبر شكل جديد من أساليب الحرب والإرهاب عبر الفضاء الالكتروني، وعلى الجانب الأخر عمل الفضاء الالكتروني على القيام بدور ايجابي على تقليل حدة الصراعات ونشر مبادرات السلام وتعزيز الحوار والتعاون بين دول العالم والانفتاح العالمي على الثقافات المختلفة .

وفي الفصل الرابع يتم تناول إمكانية تطبيق القانون الدولي على هجمات الفضاء الالكتروني بالاستناد الى مصادر القانون بالاضافة الى إلى العرف الدولي وكذلك القياس وأراء محكمة العدل الدولية بالإضافة إلى أراء الفقهاء ، و مدى امكانية تطبيق القانون الدولي الانساني و الاستفادة من قانون الفضاء الخارجي وقانون البحار ، والقانون الدولي لحقوق الإنسان. وفي الفصل الخامس يتم تناول الجهود الدولية في مكافحة الإرهاب الالكتروني على كافة المستويات سواء داخل الدول او بالتعاون مع غيرها اقليميا ، وإقرار ثقافة عالمية للأمن الالكتروني وتنتهى الرسالة بخاتمة بعنوان نحو تعزيز دور الفضاء الالكتروني في دعم السلم الدولي وتنتهي الى عدد من التوصيات من اهمها اهمية التعاون الدولي في مواجهة ظاهرة الارهاب الالكتروني و المواجهة الشاملة والموازنة بين الامن والحرية وكذلك اهمية حث الامم المتحدة والمنظمات المعنية للقيام بدورها لتحديث الاطار القانوني الدولي والسعى الى اتفاقية دولية لحماية الفضاء الالكتروني.

- **مستخلص الرسالة باللغه العربية .**

يدور موضوع هذه الدراسة حول بيان واستجلاء الآثار والتداعيات المترتبة على ظاهرة الإرهاب الالكتروني التي تنامت في ظل الثورة العلمية والمعلوماتية الحاصلة في الآونة الراهنة بالنسبة إلى استخدام القوة في العلاقات الدولية، سواء فيما يختص بعلاقة هذا بطبيعة القوة أو فيما يتعلق بمضمونها وأبعادها، ومدى تأثير ذلك كله على أنماط وحالات الصراع والسلم في العلاقات الدولية المعاصرة وخاصة ما يتعلق بتاثير ذلك على الطابع السلمي للفضاء الالكتروني كظاهرة جديدة في النظام الدولي، ومدى امكانية وجود تنظيم قانوني وثقافة عالمية لتحديد الحقوق والواجبات في استخدامه من اجل تعزيز دور الفضاء الالكتروني في دعم السلم الدولي ..

- **الكلمات الدالة:**

الأمن الرقمي – الأمن الالكتروني – الإرهاب الالكتروني – حرب المعلومات – الفضاء الالكتروني – الإرهاب الجديد – هجمات الكمبيوتر – الأمن الدولي – الانترنت – القانون الدولي – تحديات غير تقليدية – العولمة – علاقات دولية – تراث مشترك– الإرهاب عبر الانترنت – الجريمة الالكترونية – الصراع الدولي – الإرهاب – تكنولوجيا الاتصال والمعلومات – الأمم المتحدة

## The abstract

The subject of this study about the effects and elucidation the consequences of the phenomenon of cyber terrorism that have grown from the electronic revolution in scientific and information in the recently current for use the force in international relations Both in regard to the nature of this relationship of force or in regard to the content and dimensions, and the impact of all the patterns and situations of conflict and peace in the contemporary international relations.
specially as regards the impact on the peaceful nature of cyberspace as a new phenomenon in the international system and the possibility of the existence of legal regulation and and a global culture to determine the rights and obligations to use for strengthen the role of cyberspace in support of international peace



## The key words

cyber terrorism – cyber Security- a war of information - cyberspace - the new terrorism – cyber war- computers network attacks – international Security - Internet - international law- Non-traditional challenges - globalization - international relations - the common heritage - terrorism through the internet - cyber-crime - a global struggle - terrorism - information and communication technology - the United Nations

Adel abdel sadek Mohamed Algakha
Monofia
Egyptian

# The Impact of Cyber Terrorism on Use the Force in International Relation (2001-2007)

Under The Supervision
**Prof. Ahmed Abdel Wanis Sheta**

The summary

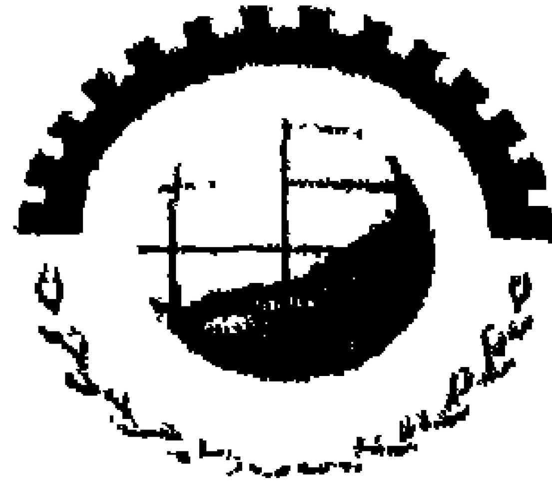
The phenomenon of cyberspace on the positive repercussions of the international community, represented important role in the evolution of the international community, while at the same time, the phenomenon reflected the growing role of international accreditation with the increase in the levels of all the political, economic, security, cultural and other, reflecting the phenomenon of multi-dimensional interests include electronic and at the same time exposed to the dangers of email and the technological revolution and the emergence of community risk in the international system, and there was the nature of electronic security, power and conflict in the international system, and the impact of space electronic interactions on the international political and democratic change.

In chapter II, a researcher said in spite of the cyber terrorism discriminate in terms of concept and its characteristics and its mechanisms, however, it raises another set of concepts, which differed from the cyber terrorism it - at the same time - linked to one degree or another.

In chapter III, will be addressing the role of cyberspace in influencing the nature of the conflict and power, exercised through as well as to the nature of the results and effects that result, and this is reflected by a new type of exercise of power and attack and defense through a new form of methods of warfare and terrorism through cyberspace and on the other side the work of cyberspace to play a positive role in reducing conflicts and the deployment of peace initiatives and the promotion of dialogue and cooperation between the countries of the world and opening up to the world of different cultures.

In the fourth chapter would be taken up the applicability of international law to cyberspace attacks based on the sources of law as well as to international custom, as well as measurement and the views of the International Court of Justice in addition to the views of scholars, and the possibility of the application of international humanitarian law and take advantage of the Law of Outer Space and the Law of the Sea, and the law international human rights.

In chapter V, would be taken up international efforts to combat terrorism at all levels both within the state or in cooperation with other regional and the adoption of a global culture of security of the electronic message and ends on a note of the title towards the strengthening of the role of cyberspace in support of international peace and end to a number of recommendations, most important of the importance of cooperation international phenomenon of terrorism in the face of the balance between security and liberty, as well as the importance of urging the United Nations and relevant organizations to do its part to modernize the international legal framework and to seek an international convention for the protection of cyberspace.



Cairo University
Faculty of Economic and Political Science

# The Impact of Cyber Terrorism on Use the Force in International Relation (2001-2007)

A Thesis Submitted in Partial Fulfillment of the Requirements for the Master In Political Science

By

**Adel Abdel Sadek Mohammed Algakha**

Under The Supervision

**Prof. Ahmed Abdel Wanis Sheta**
Professor of Political Science and International law

Cairo

2009